OIPE IAP21
NOV 06 2006
PATENT & TRADEMARK OFFICE

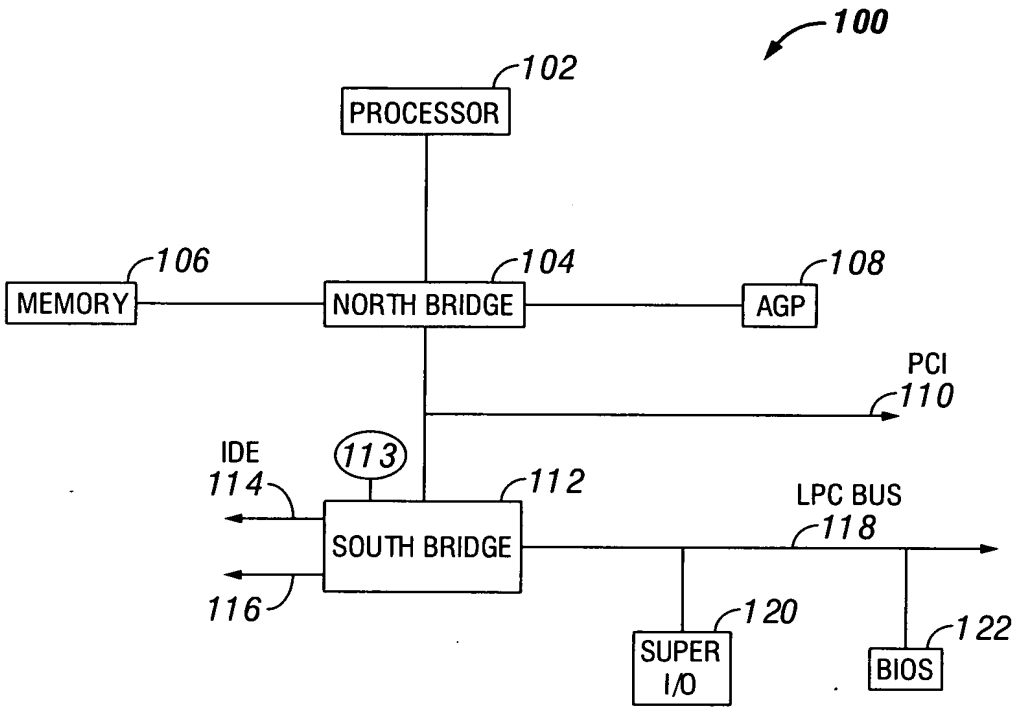

FIG. 1A
(Prior Art)

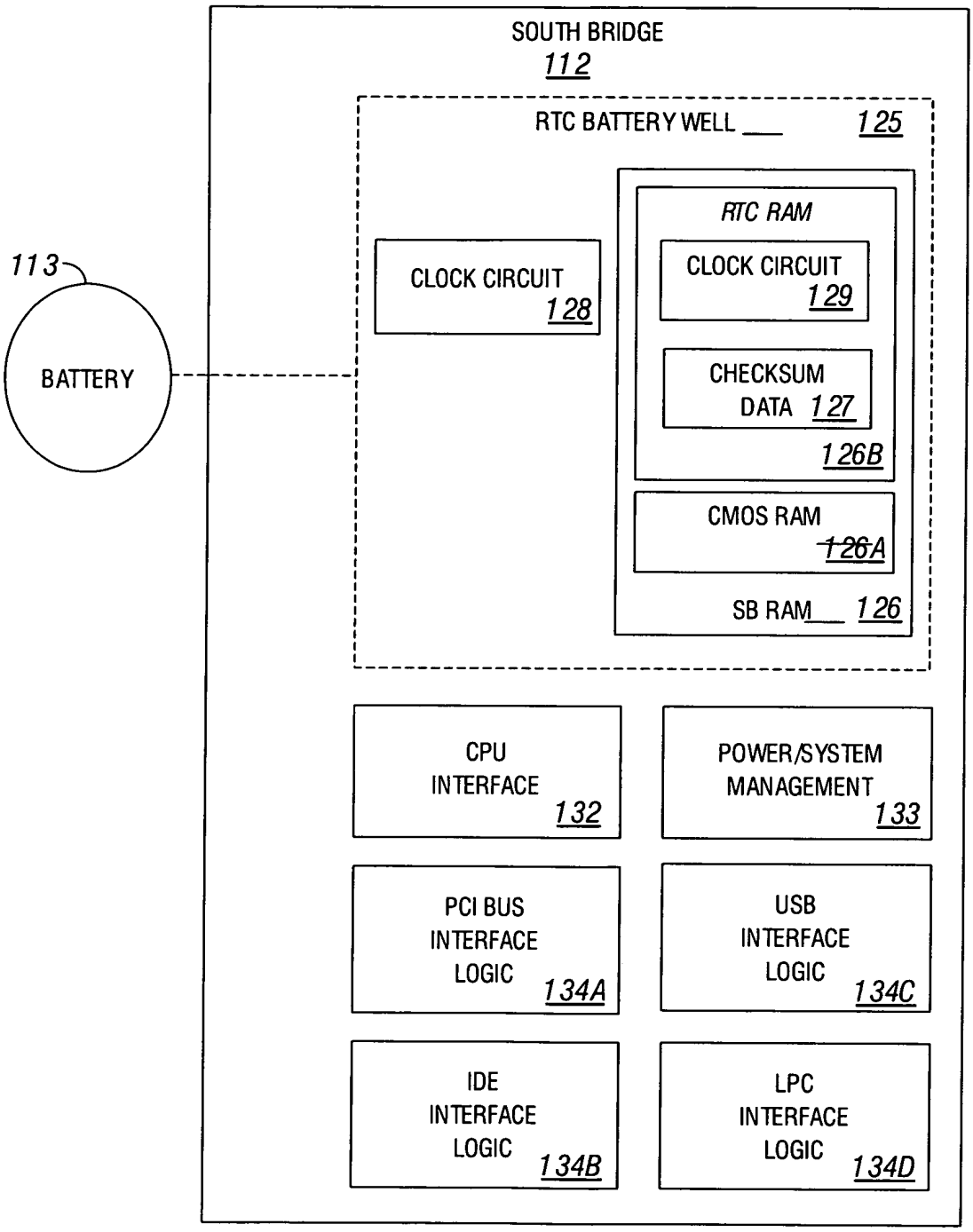

FIG. 1B
(Prior Art)

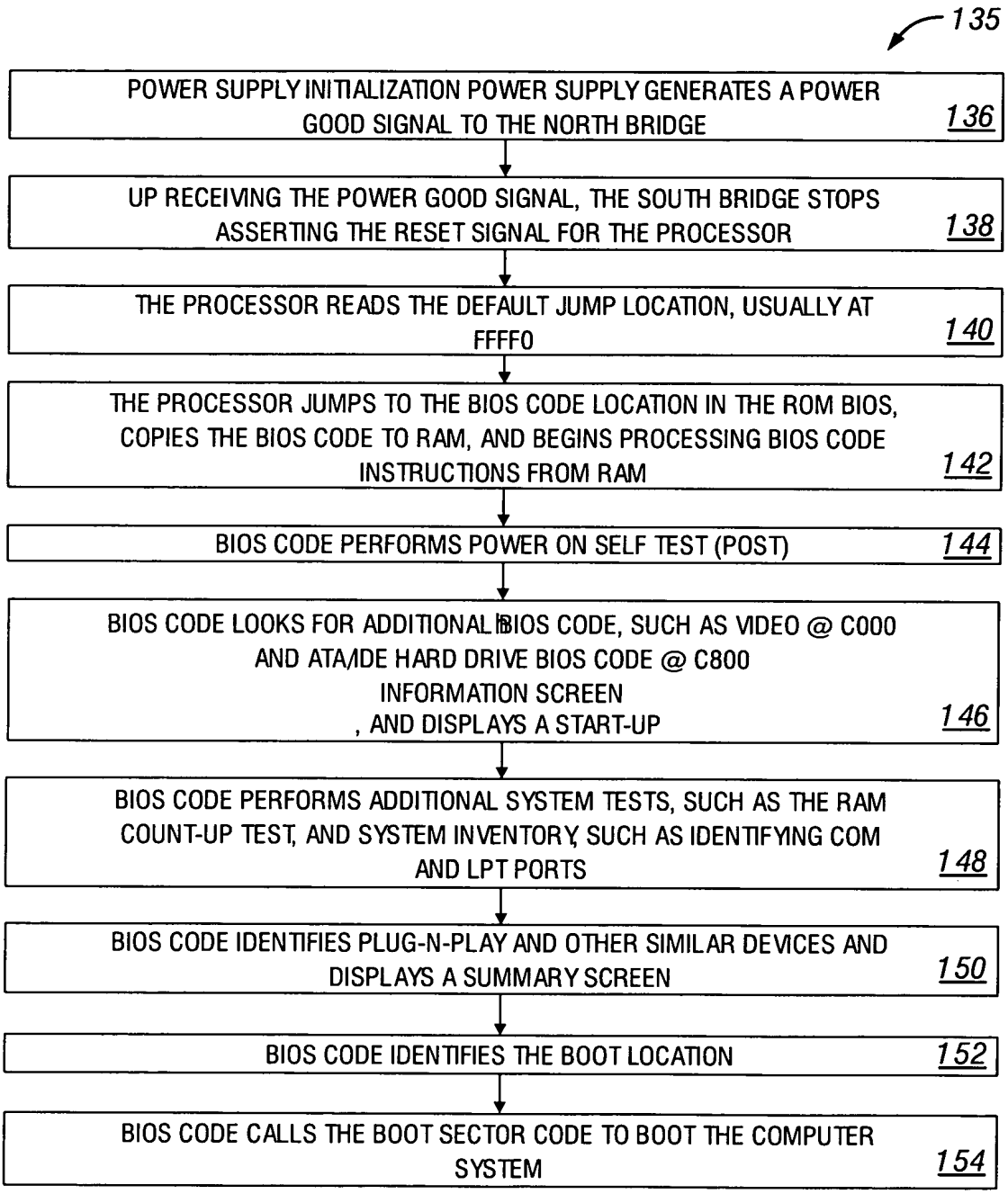

FIG. 2A
(Prior Art)

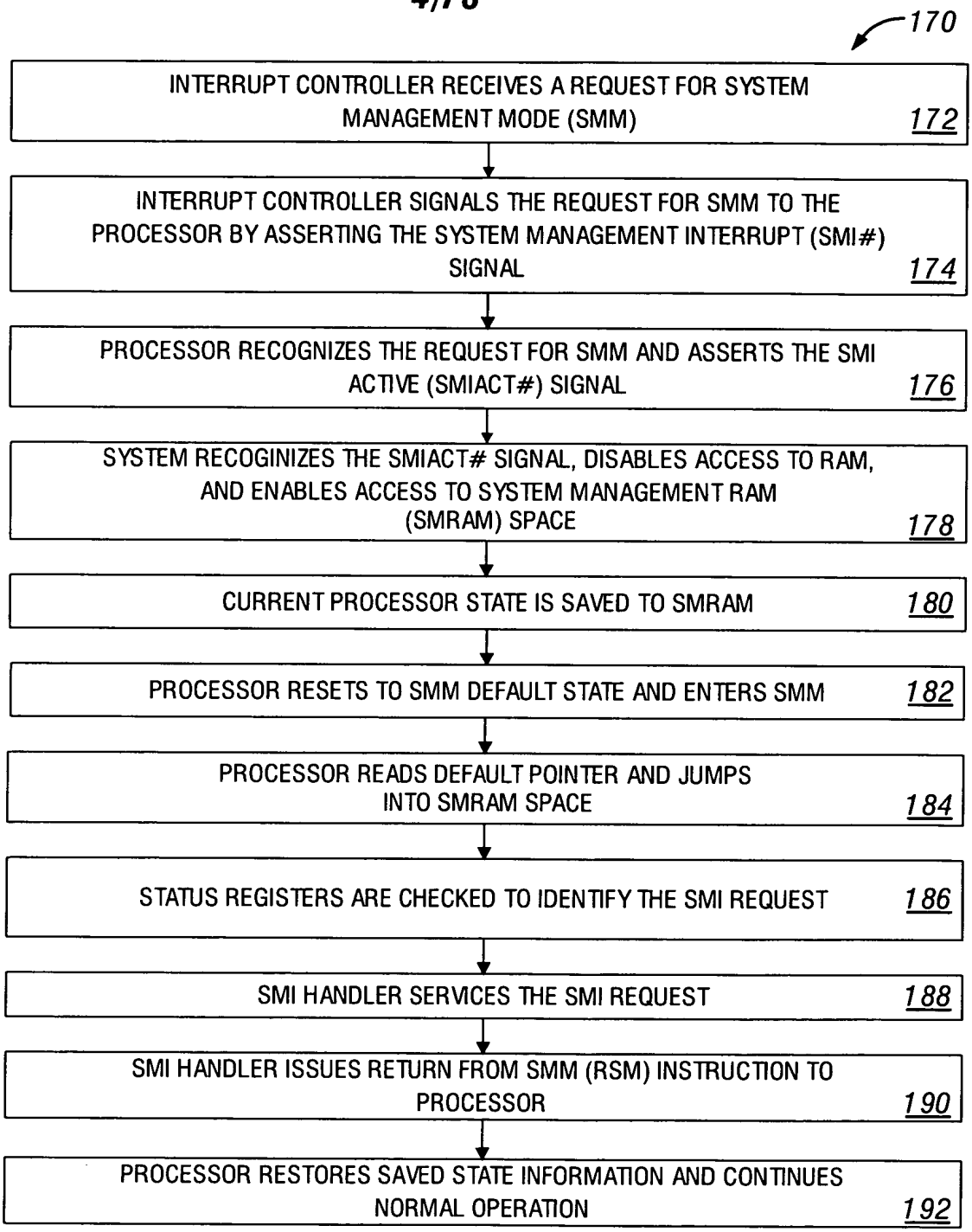

FIG. 2B
(Prior Art)

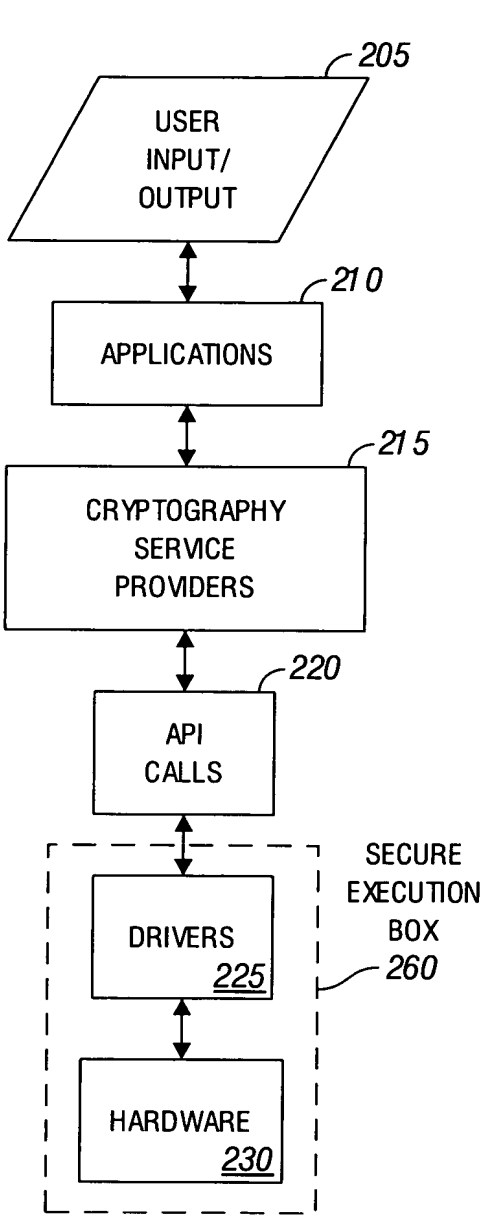
200
205
USER INPUT/ OUTPUT
210
APPLICATIONS
215
CRYPTOGRAPHY SERVICE PROVIDERS
220
API CALLS
SECURE EXECUTION BOX
260
DRIVERS 225
HARDWARE 230

FIG. 3

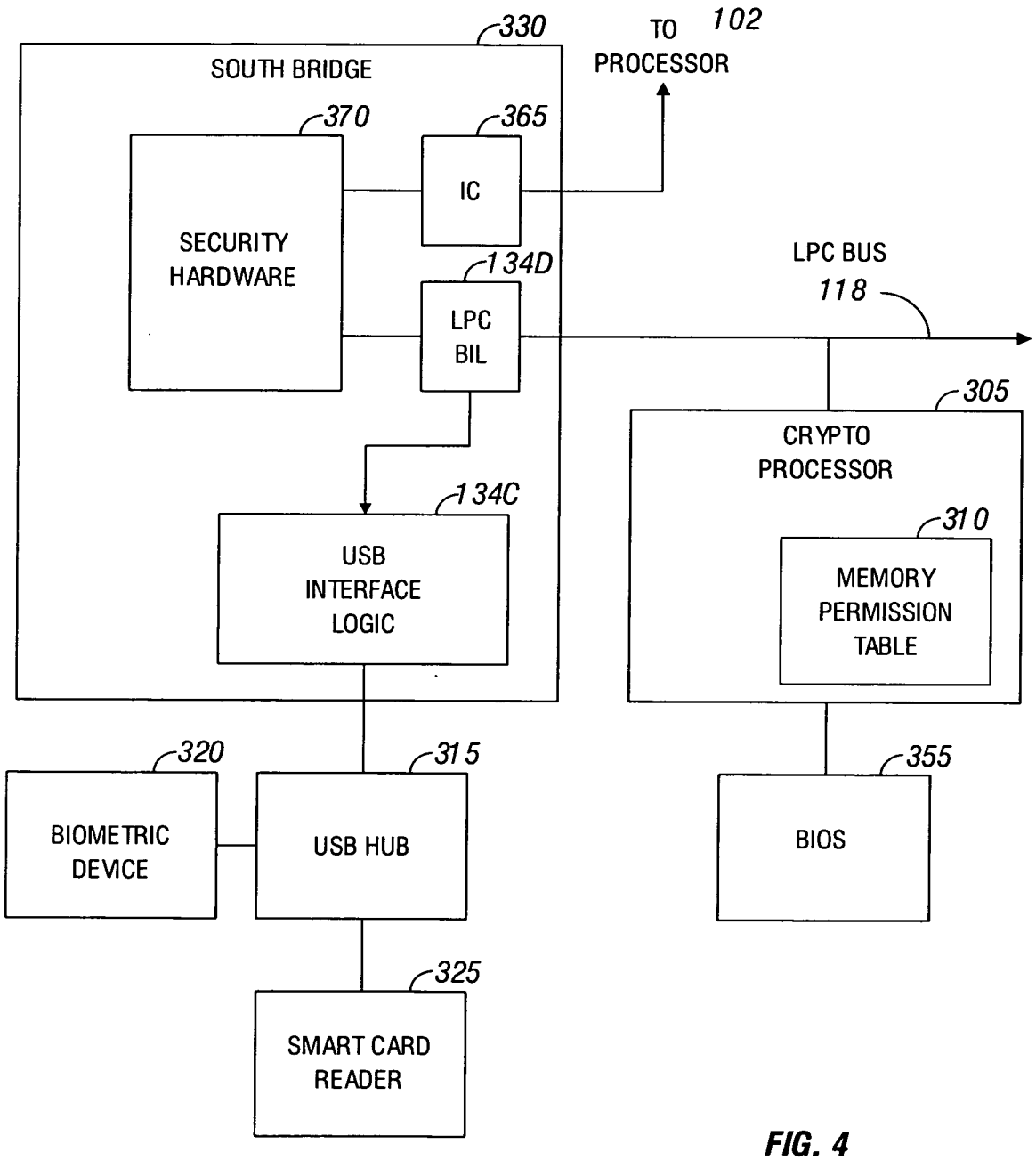
330
SOUTH BRIDGE
TO PROCESSOR
102
370
365
SECURITY HARDWARE
IC
134D
LPC BIL
LPC BUS
118
305
CRYPTO PROCESSOR
134C
310
USB INTERFACE LOGIC
MEMORY PERMISSION TABLE
320
315
355
BIOMETRIC DEVICE
USB HUB
BIOS
325
SMART CARD READER

FIG. 4

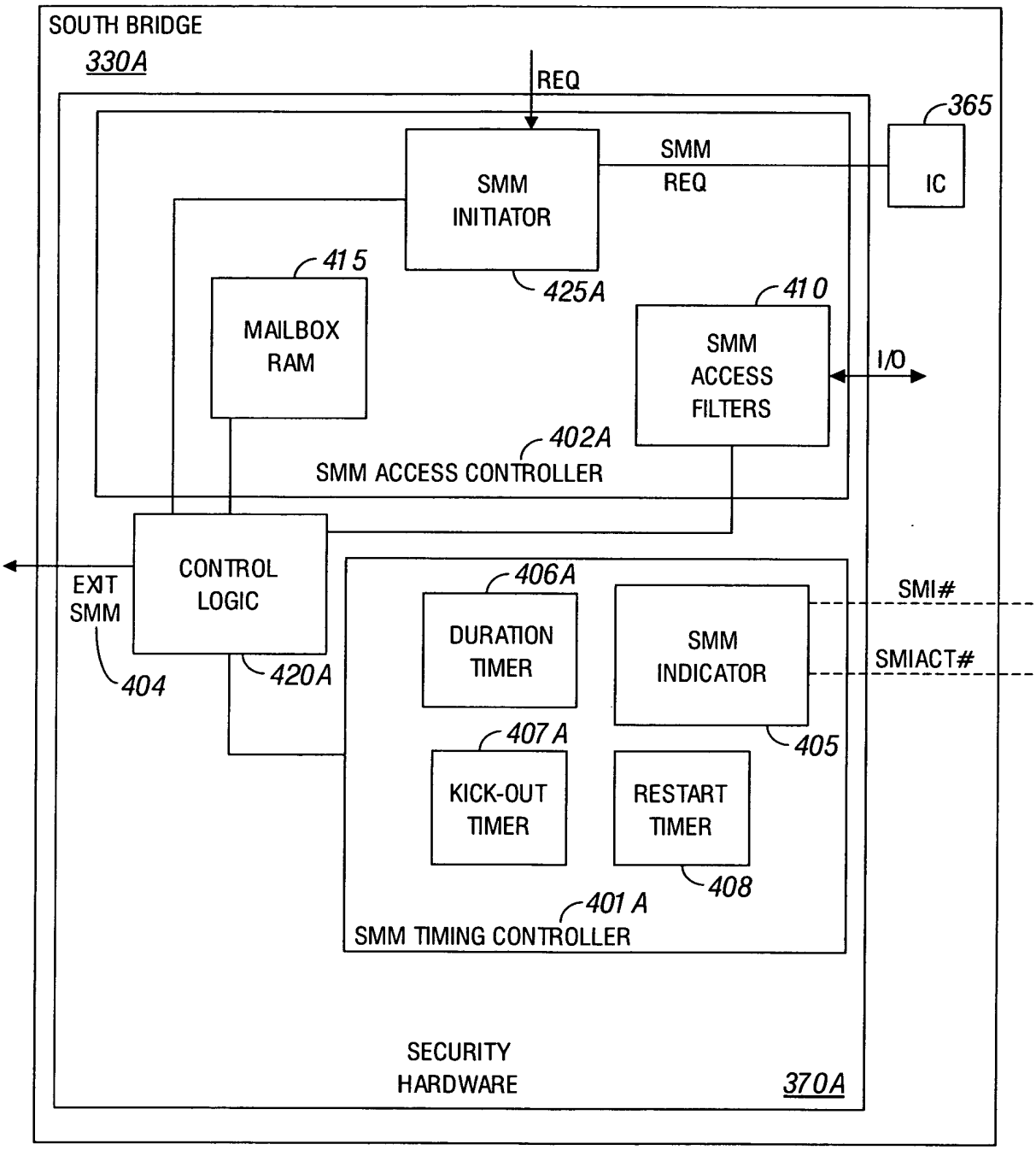
SOUTH BRIDGE
330A
REQ
365
SMM
REQ
IC
SMM
INITIATOR
425A
415
MAILBOX
RAM
410
SMM
ACCESS
FILTERS
I/O
402A
SMM ACCESS CONTROLLER
CONTROL
LOGIC
EXT
SMM
404
420A
406A
DURATION
TIMER
SMM
INDICATOR
SMI#
SMIACT#
405
407A
KICK-OUT
TIMER
RESTART
TIMER
408
401A
SMM TIMING CONTROLLER
SECURITY
HARDWARE
370A

FIG. 5A

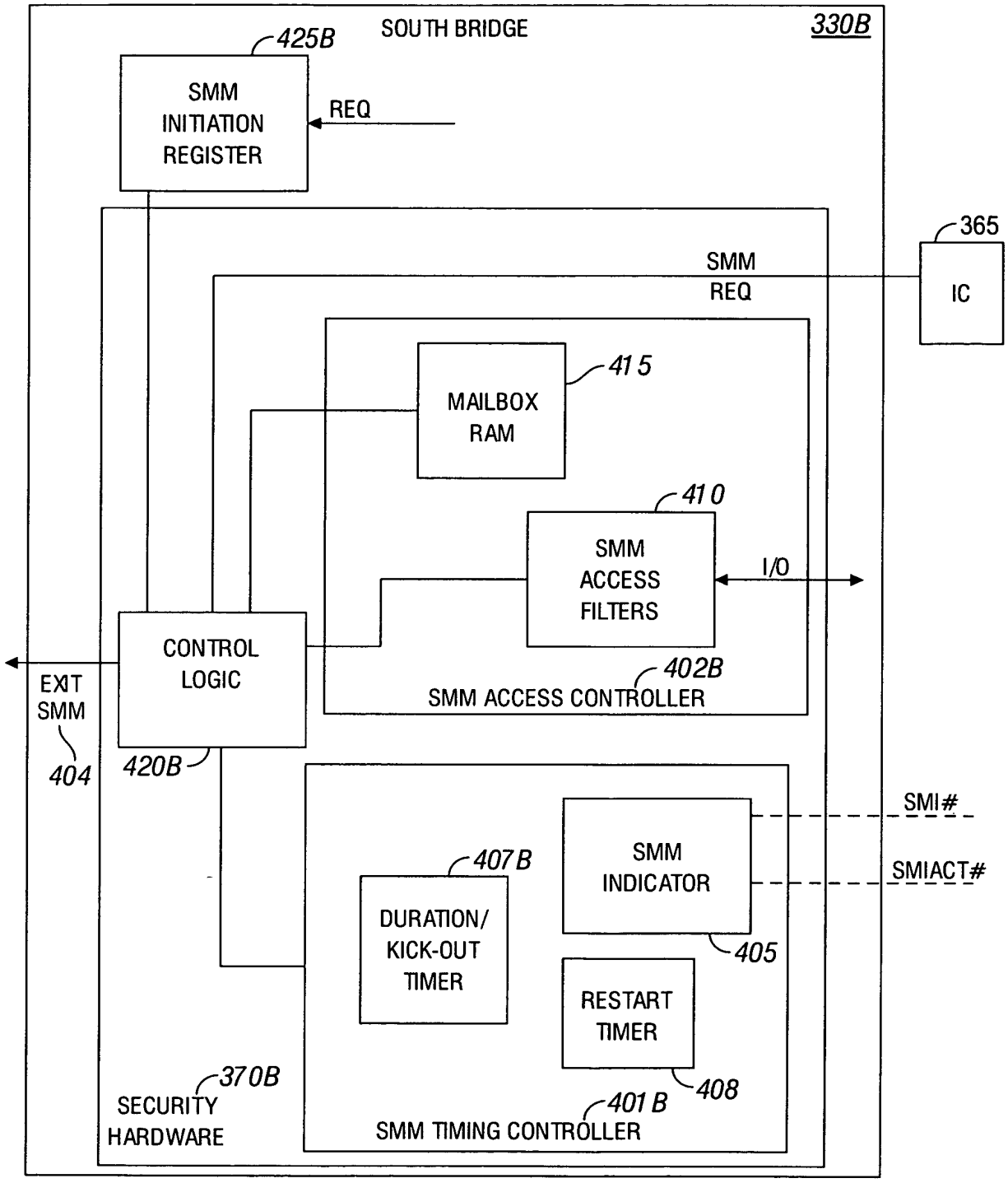
SOUTH BRIDGE
330B
425B
SMM INITIATION REGISTER
REQ
365
IC
SMM REQ
MAILBOX RAM
415
410
SMM ACCESS FILTERS
I/O
CONTROL LOGIC
EXIT SMM
404
420B
402B
SMM ACCESS CONTROLLER
SMI#
SMIACT#
SMM INDICATOR
405
407B
DURATION/ KICK-OUT TIMER
RESTART TIMER
408
401B
SMM TIMING CONTROLLER
370B
SECURITY HARDWARE

FIG. 5B

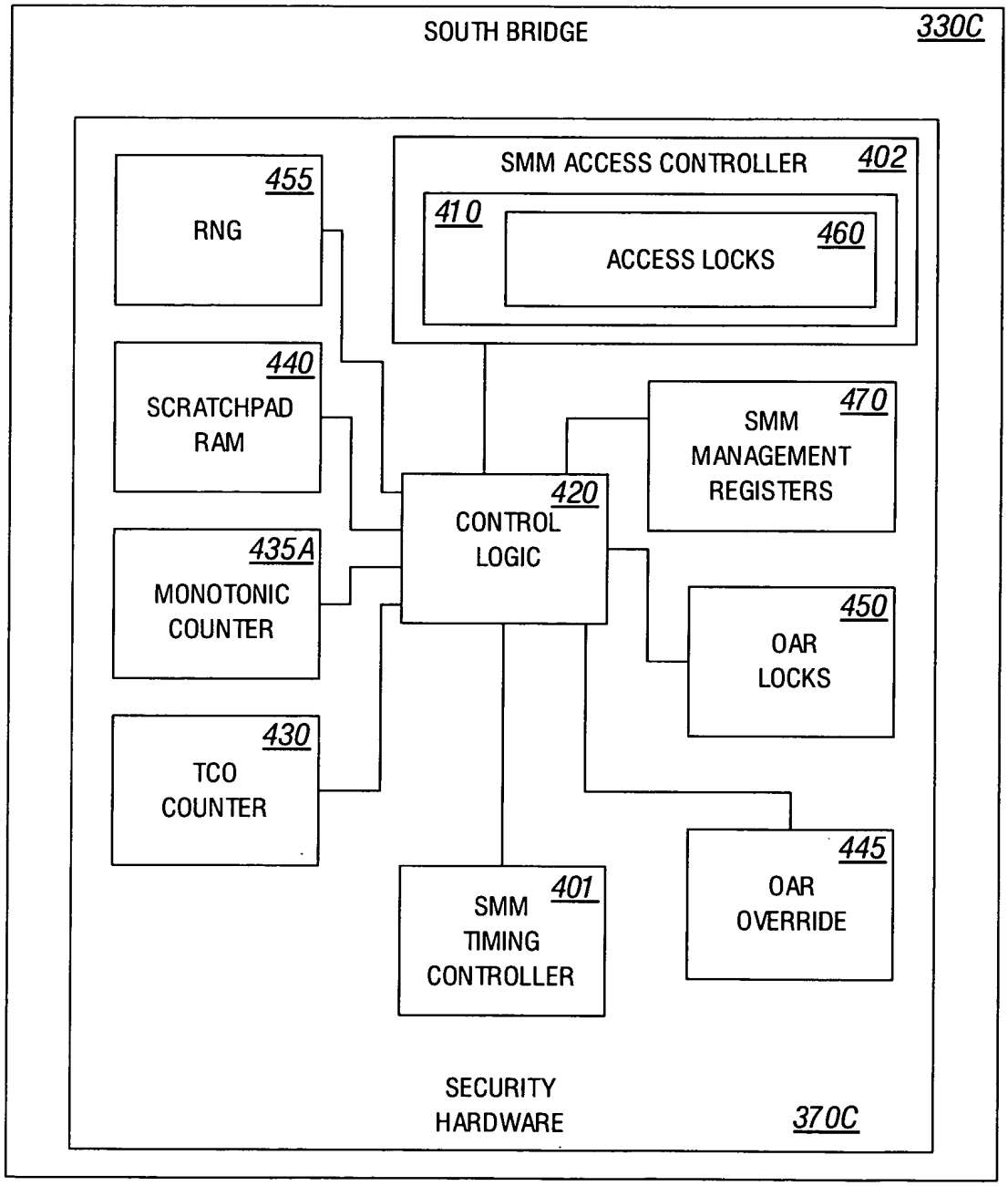
SOUTH BRIDGE
330C
SMM ACCESS CONTROLLER
402
410
460
ACCESS LOCKS
455
RNG
440
SCRATCHPAD RAM
470
SMM MANAGEMENT REGISTERS
420
CONTROL LOGIC
435A
MONOTONIC COUNTER
450
OAR LOCKS
430
TCO COUNTER
445
OAR OVERRIDE
401
SMM TIMING CONTROLLER
SECURITY HARDWARE
370C

FIG. 6

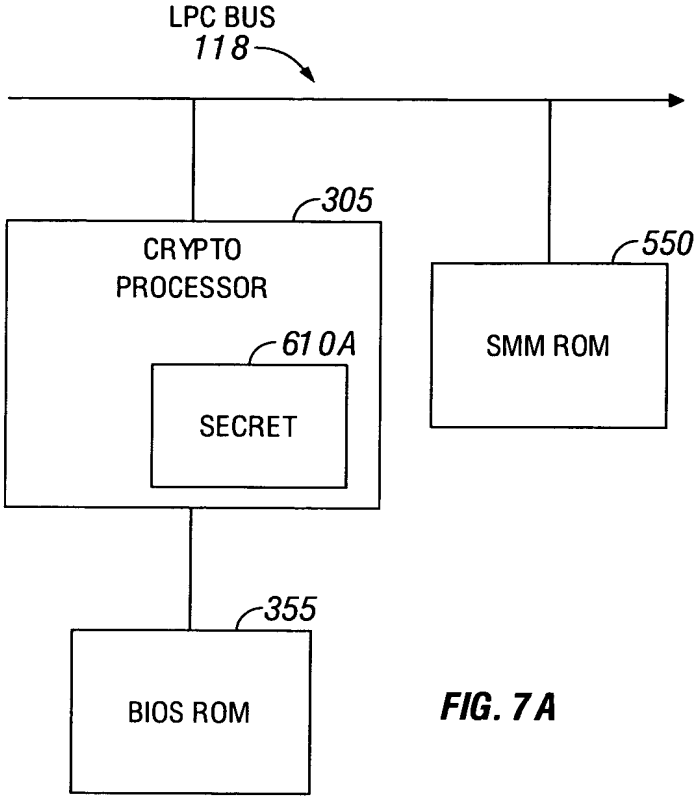
LPC BUS
118
305
CRYPTO
PROCESSOR
610A
SECRET
550
SMM ROM
355
BIOS ROM

FIG. 7A

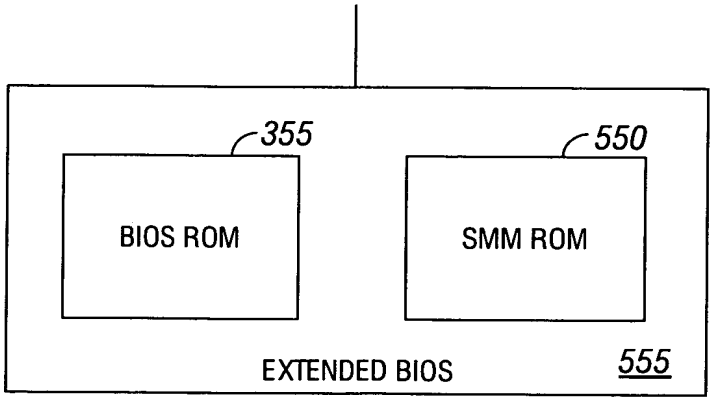
355
BIOS ROM
550
SMM ROM
EXTENDED BIOS
555

FIG. 7B

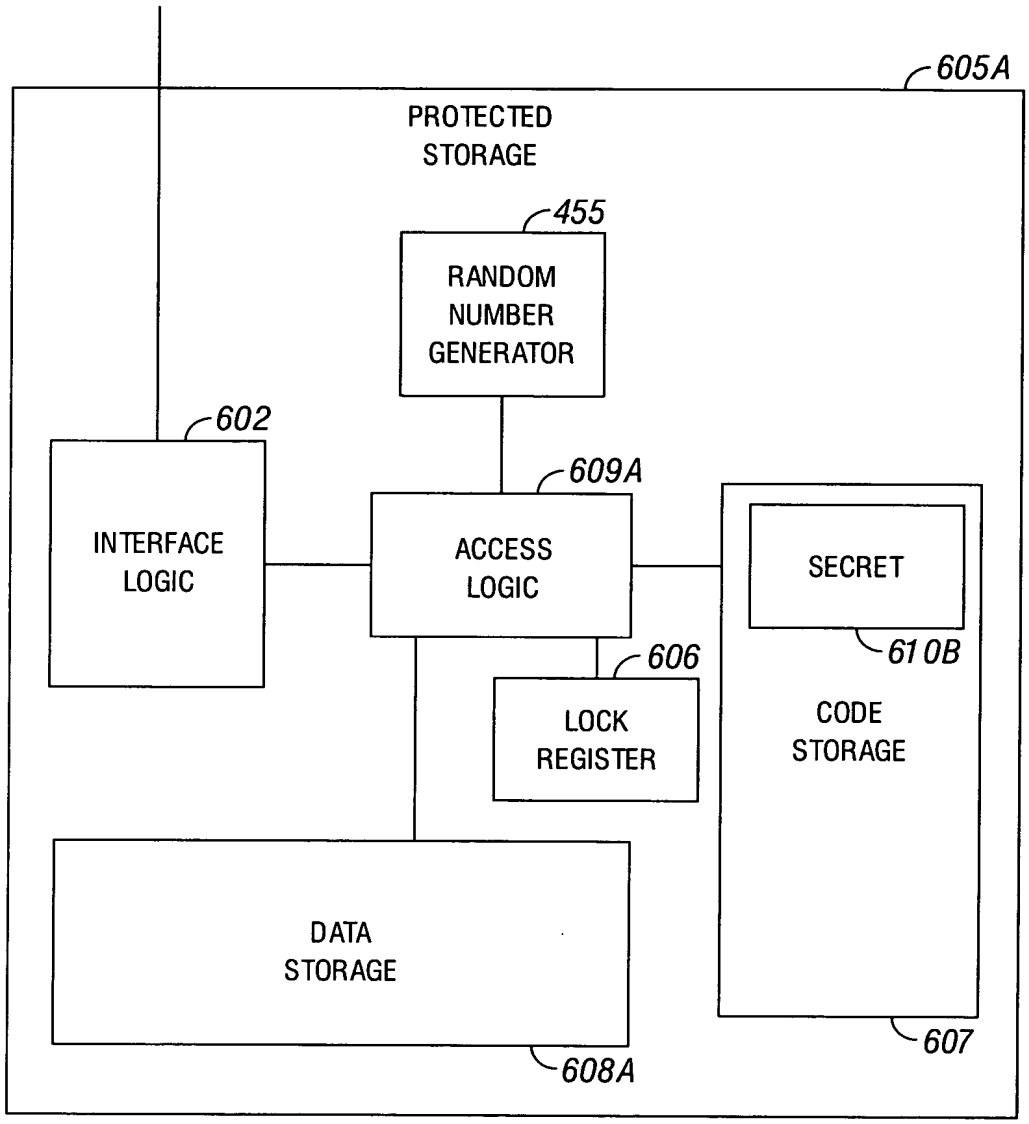
605A
PROTECTED STORAGE
455
RANDOM NUMBER GENERATOR
602
INTERFACE LOGIC
609A
ACCESS LOGIC
SECRET
610B
606
LOCK REGISTER
CODE STORAGE
DATA STORAGE
608A
607

FIG. 7C

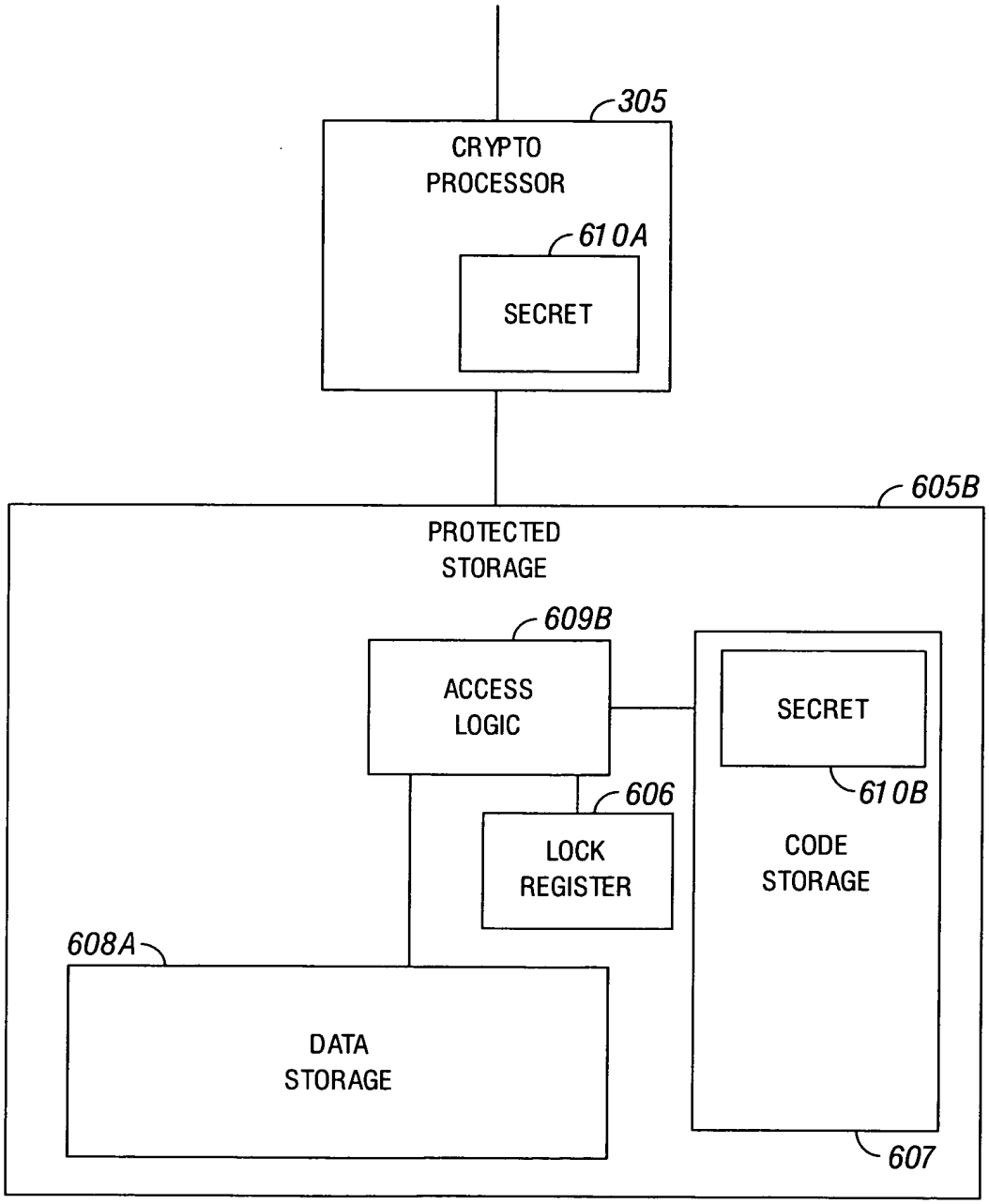
305
CRYPTO
PROCESSOR
610A
SECRET
605B
PROTECTED
STORAGE
609B
ACCESS
LOGIC
606
LOCK
REGISTER
608A
DATA
STORAGE
SECRET
610B
CODE
STORAGE
607

FIG. 7D

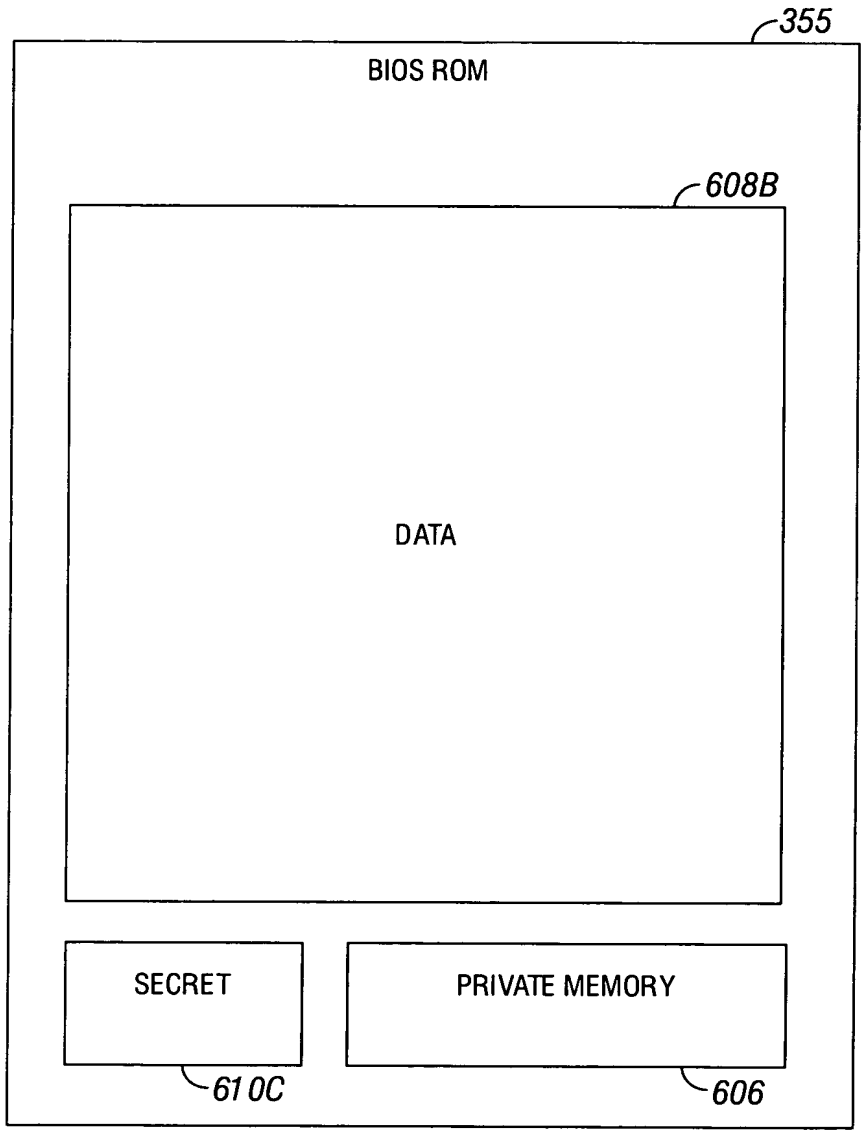

FIG. 8A

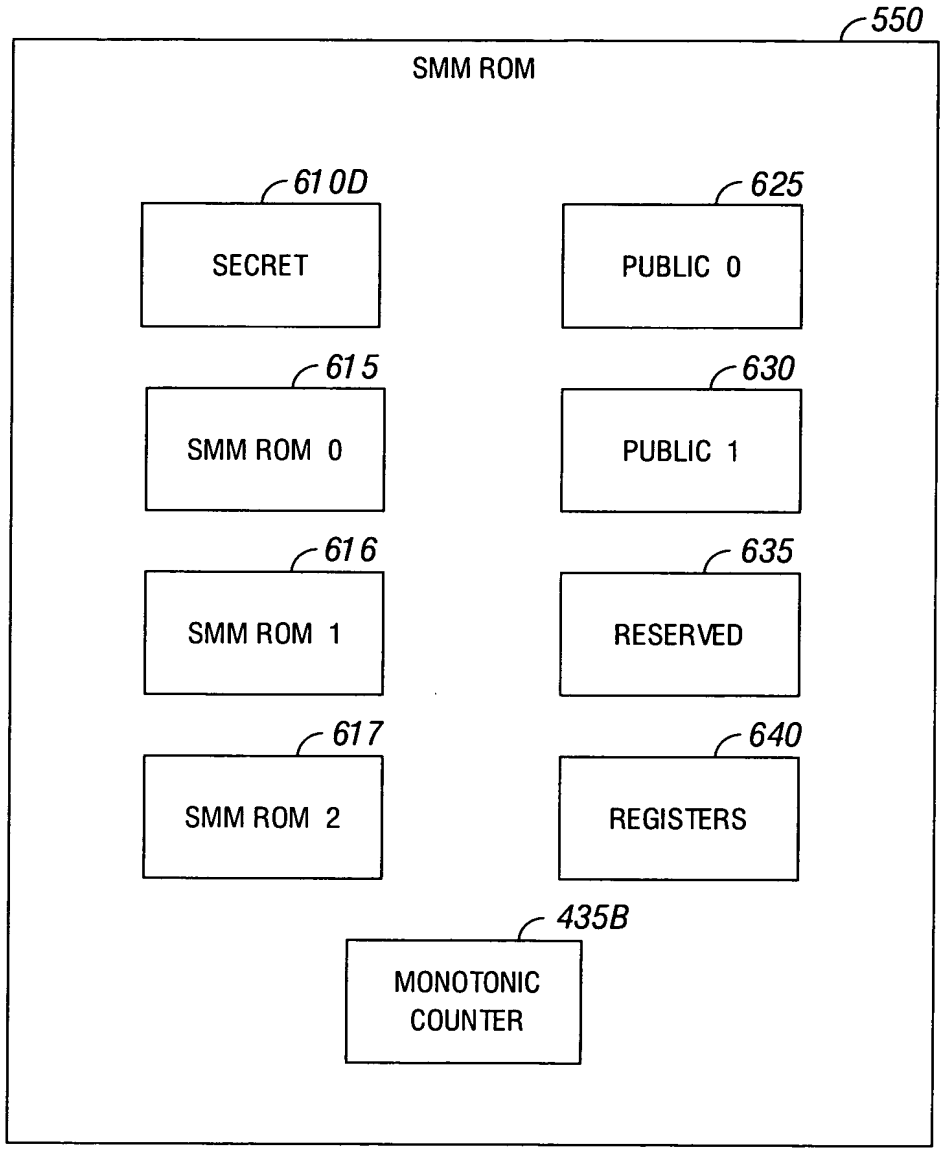
550
SMM ROM
610D
SECRET
625
PUBLIC 0
615
SMM ROM 0
630
PUBLIC 1
616
SMM ROM 1
635
RESERVED
617
SMM ROM 2
640
REGISTERS
435B
MONOTONIC COUNTER

FIG. 8B

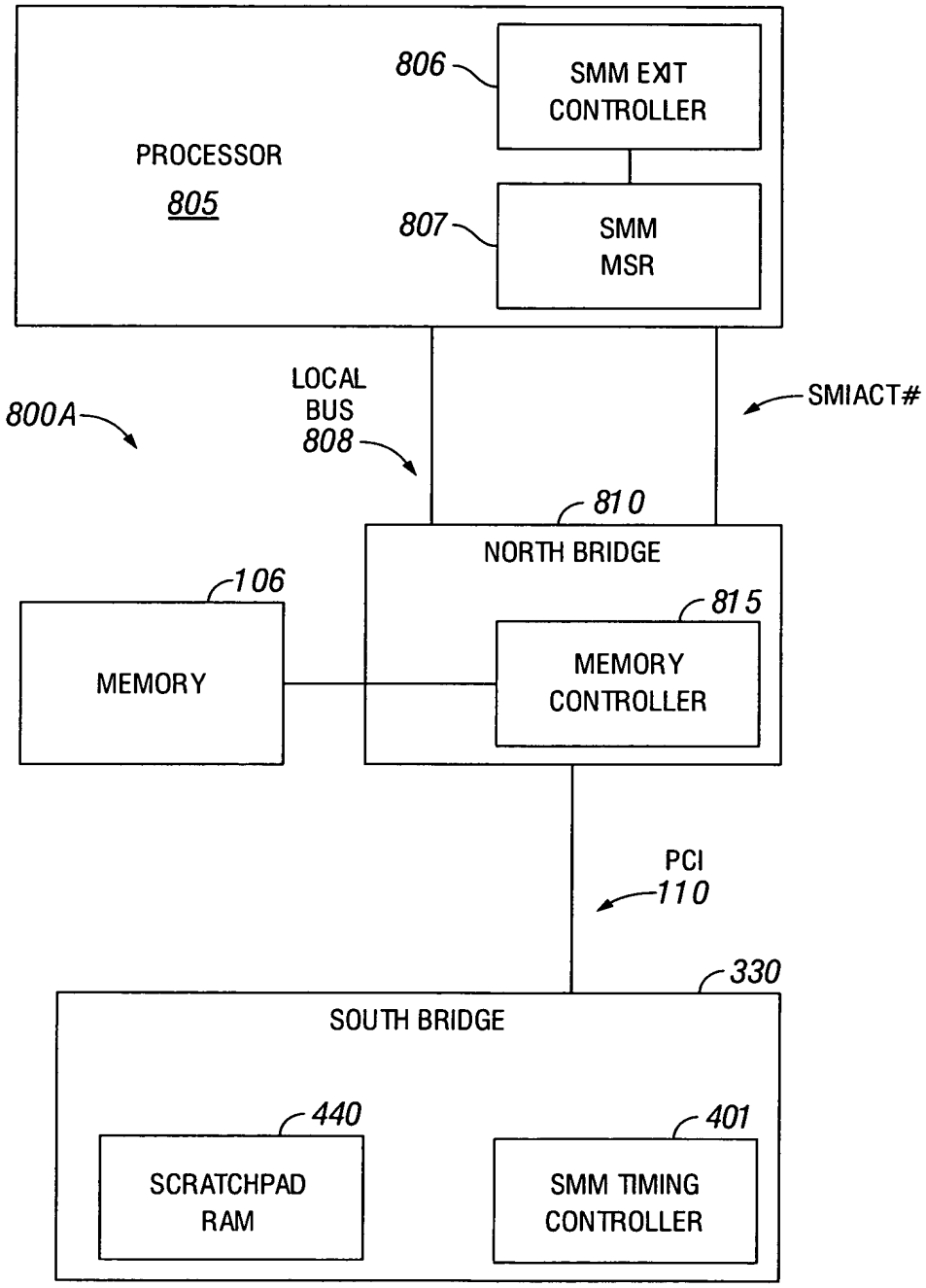
806
SMM EXIT CONTROLLER
PROCESSOR
805
807
SMM MSR
LOCAL BUS
808
800A
SMIACT#
810
NORTH BRIDGE
106
MEMORY
815
MEMORY CONTROLLER
PCI
110
330
SOUTH BRIDGE
440
SCRATCHPAD RAM
401
SMM TIMING CONTROLLER

FIG. 9A

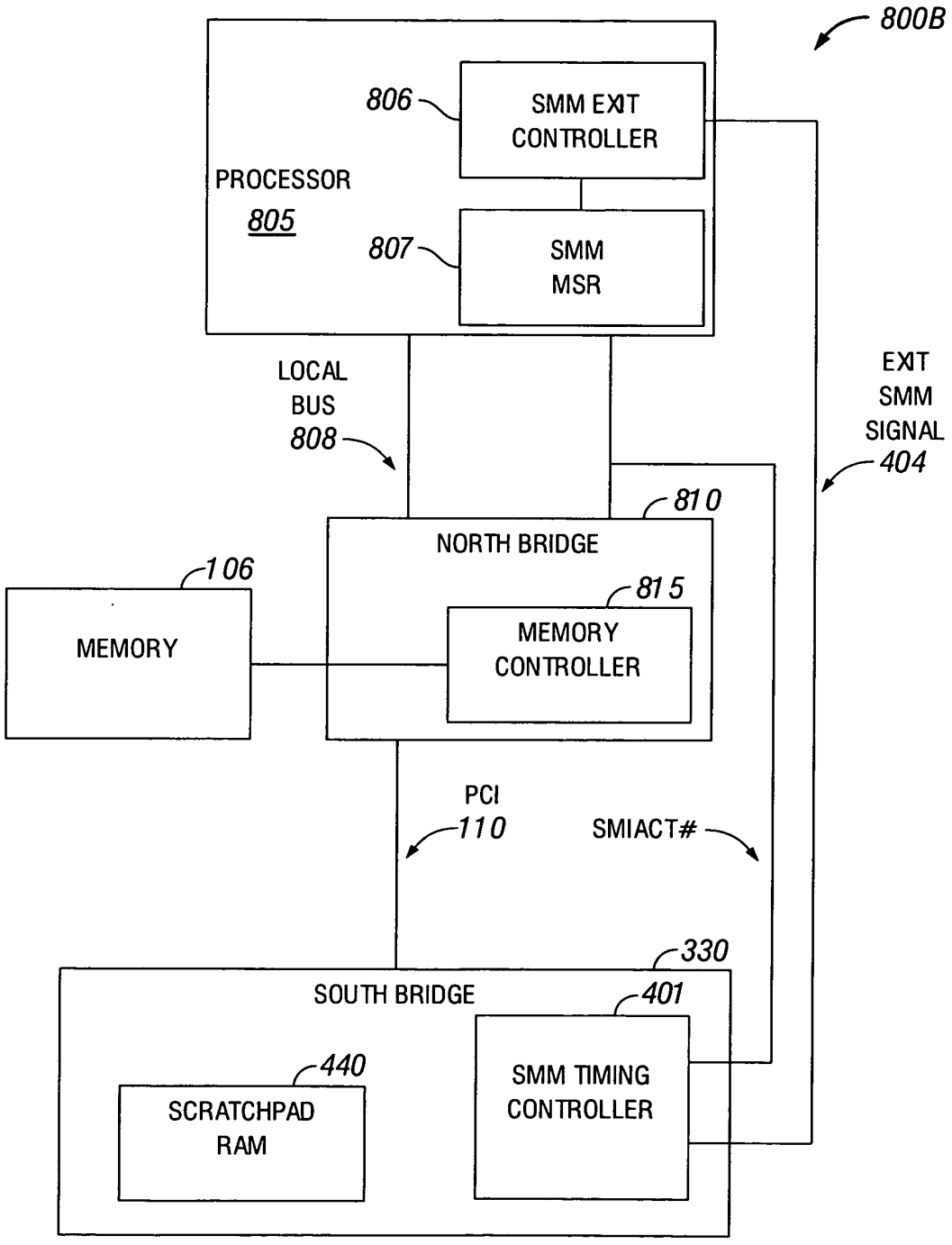
800B
806
SMM EXIT CONTROLLER
PROCESSOR
805
807
SMM MSR
LOCAL BUS
808
EXIT SMM SIGNAL
404
810
NORTH BRIDGE
106
MEMORY
815
MEMORY CONTROLLER
PCI
110
SMIACT#
330
SOUTH BRIDGE
401
440
SCRATCHPAD RAM
SMM TIMING CONTROLLER

FIG. 9B

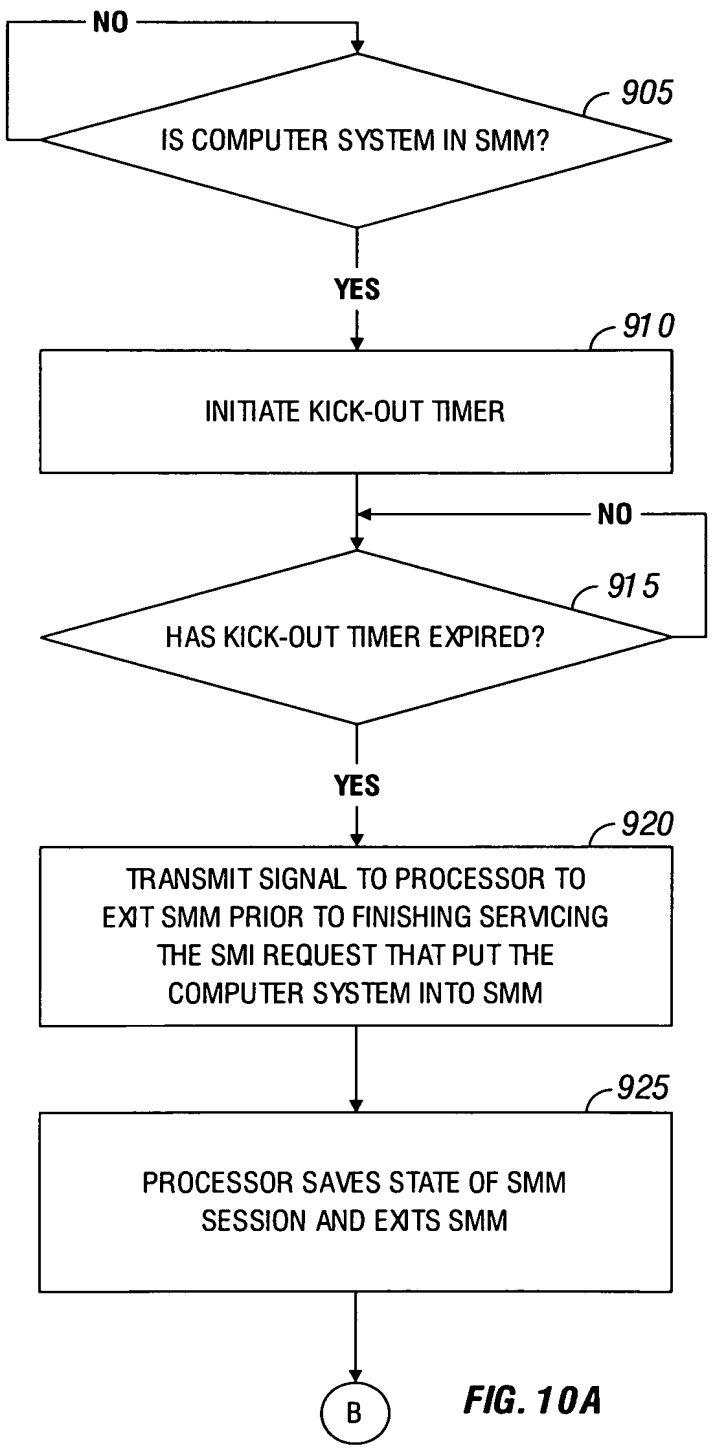
900
NO
905
IS COMPUTER SYSTEM IN SMM?
YES
910
INITIATE KICK-OUT TIMER
NO
915
HAS KICK-OUT TIMER EXPIRED?
YES
920
TRANSMIT SIGNAL TO PROCESSOR TO EXIT SMM PRIOR TO FINISHING SERVICING THE SMI REQUEST THAT PUT THE COMPUTER SYSTEM INTO SMM
925
PROCESSOR SAVES STATE OF SMM SESSION AND EXITS SMM
B

FIG. 10A

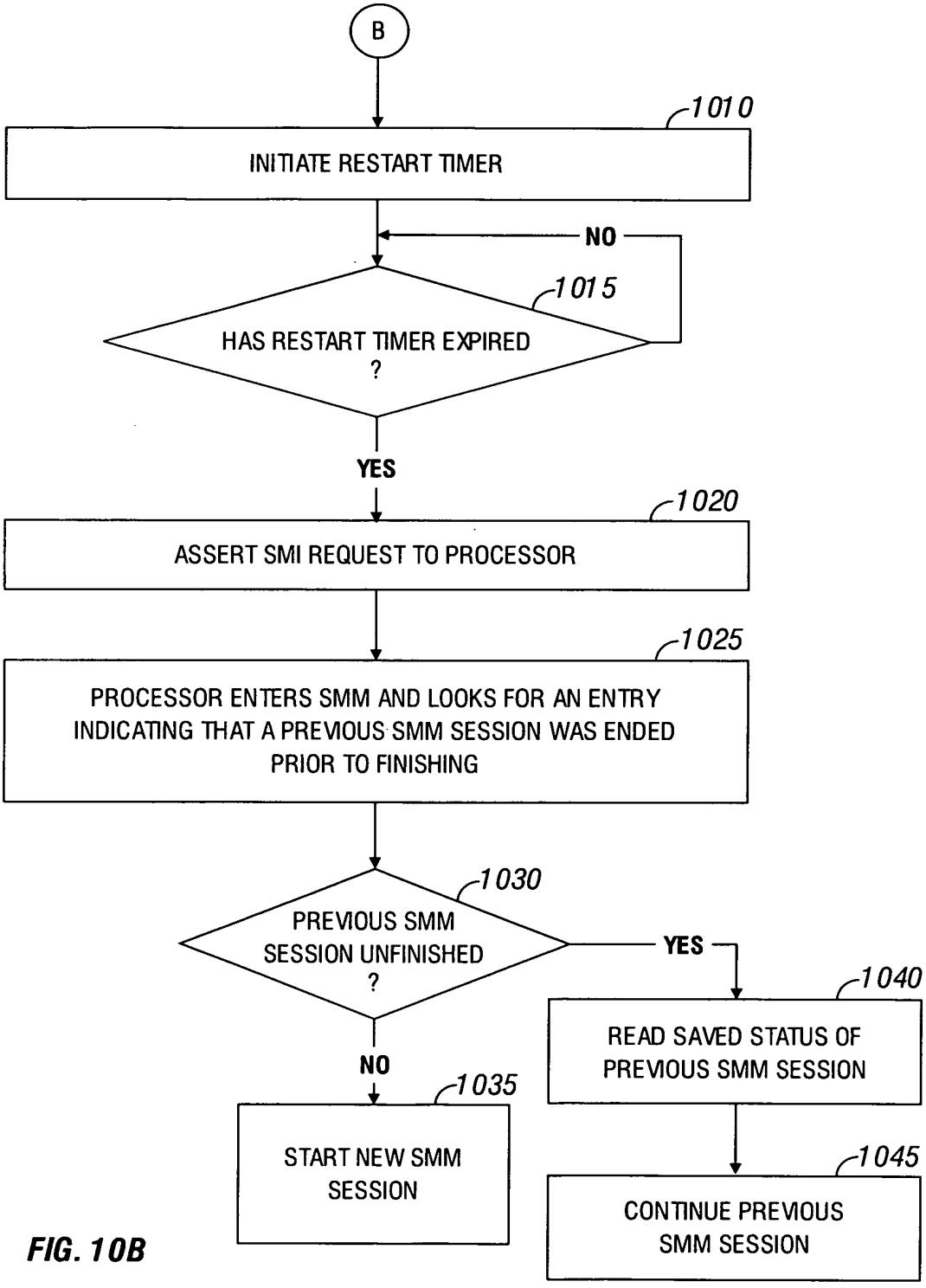
B
1010
INITIATE RESTART TIMER
NO
1015
HAS RESTART TIMER EXPIRED ?
YES
1020
ASSERT SMI REQUEST TO PROCESSOR
1025
PROCESSOR ENTERS SMM AND LOOKS FOR AN ENTRY INDICATING THAT A PREVIOUS SMM SESSION WAS ENDED PRIOR TO FINISHING
1030
PREVIOUS SMM SESSION UNFINISHED ?
YES
1040
READ SAVED STATUS OF PREVIOUS SMM SESSION
NO
1035
START NEW SMM SESSION
1045
CONTINUE PREVIOUS SMM SESSION

FIG. 10B

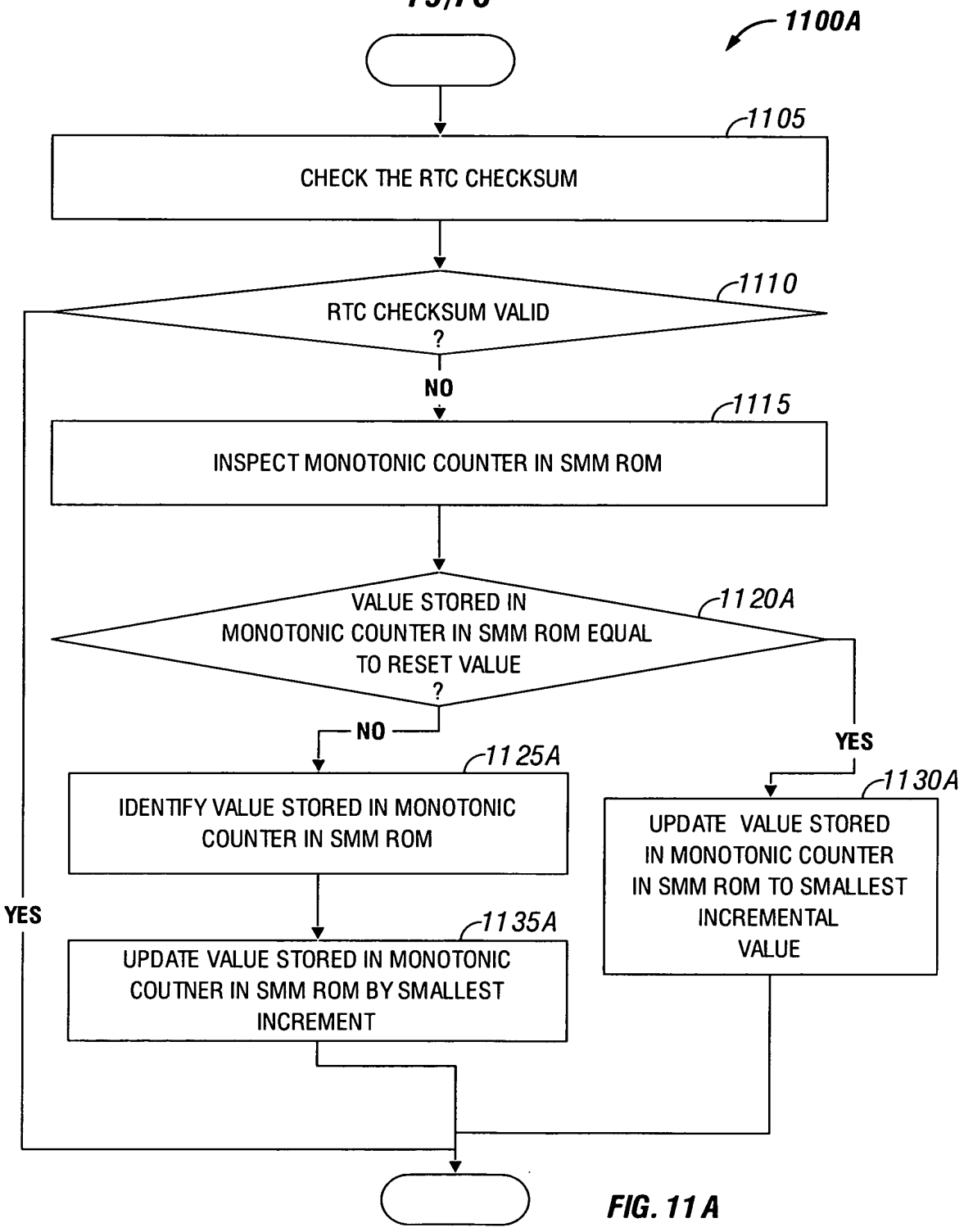
1100A
1105
CHECK THE RTC CHECKSUM
1110
RTC CHECKSUM VALID ?
NO
1115
INSPECT MONOTONIC COUNTER IN SMM ROM
1120A
VALUE STORED IN MONOTONIC COUNTER IN SMM ROM EQUAL TO RESET VALUE ?
NO
YES
1125A
IDENTIFY VALUE STORED IN MONOTONIC COUNTER IN SMM ROM
1130A
UPDATE VALUE STORED IN MONOTONIC COUNTER IN SMM ROM TO SMALLEST INCREMENTAL VALUE
YES
1135A
UPDATE VALUE STORED IN MONOTONIC COUTNER IN SMM ROM BY SMALLEST INCREMENT

FIG. 11A

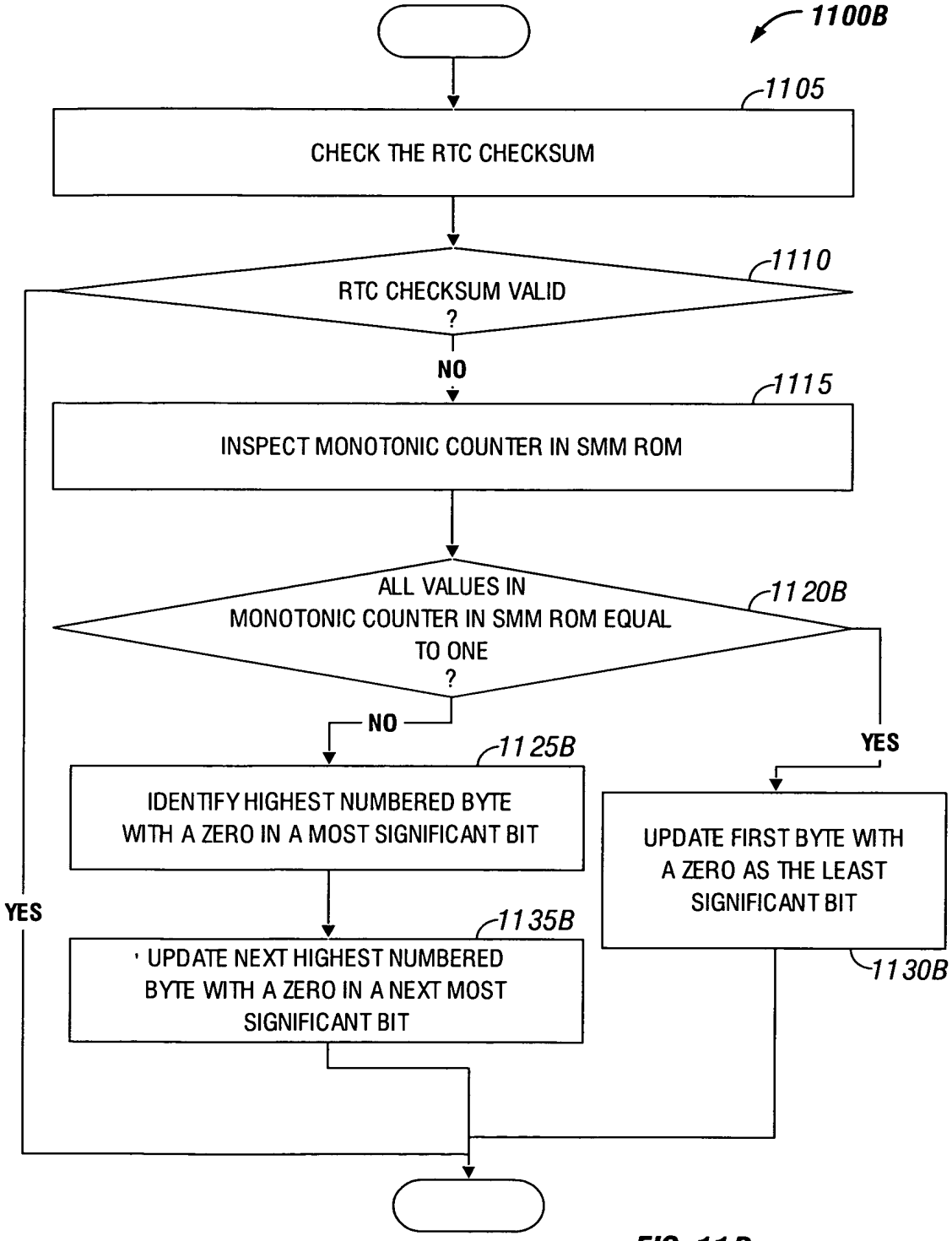
1100B
1105
CHECK THE RTC CHECKSUM
1110
RTC CHECKSUM VALID ?
NO
YES
1115
INSPECT MONOTONIC COUNTER IN SMM ROM
1120B
ALL VALUES IN MONOTONIC COUNTER IN SMM ROM EQUAL TO ONE ?
NO
YES
1125B
IDENTIFY HIGHEST NUMBERED BYTE WITH A ZERO IN A MOST SIGNIFICANT BIT
1135B
UPDATE NEXT HIGHEST NUMBERED BYTE WITH A ZERO IN A NEXT MOST SIGNIFICANT BIT
UPDATE FIRST BYTE WITH A ZERO AS THE LEAST SIGNIFICANT BIT
1130B

FIG. 11B

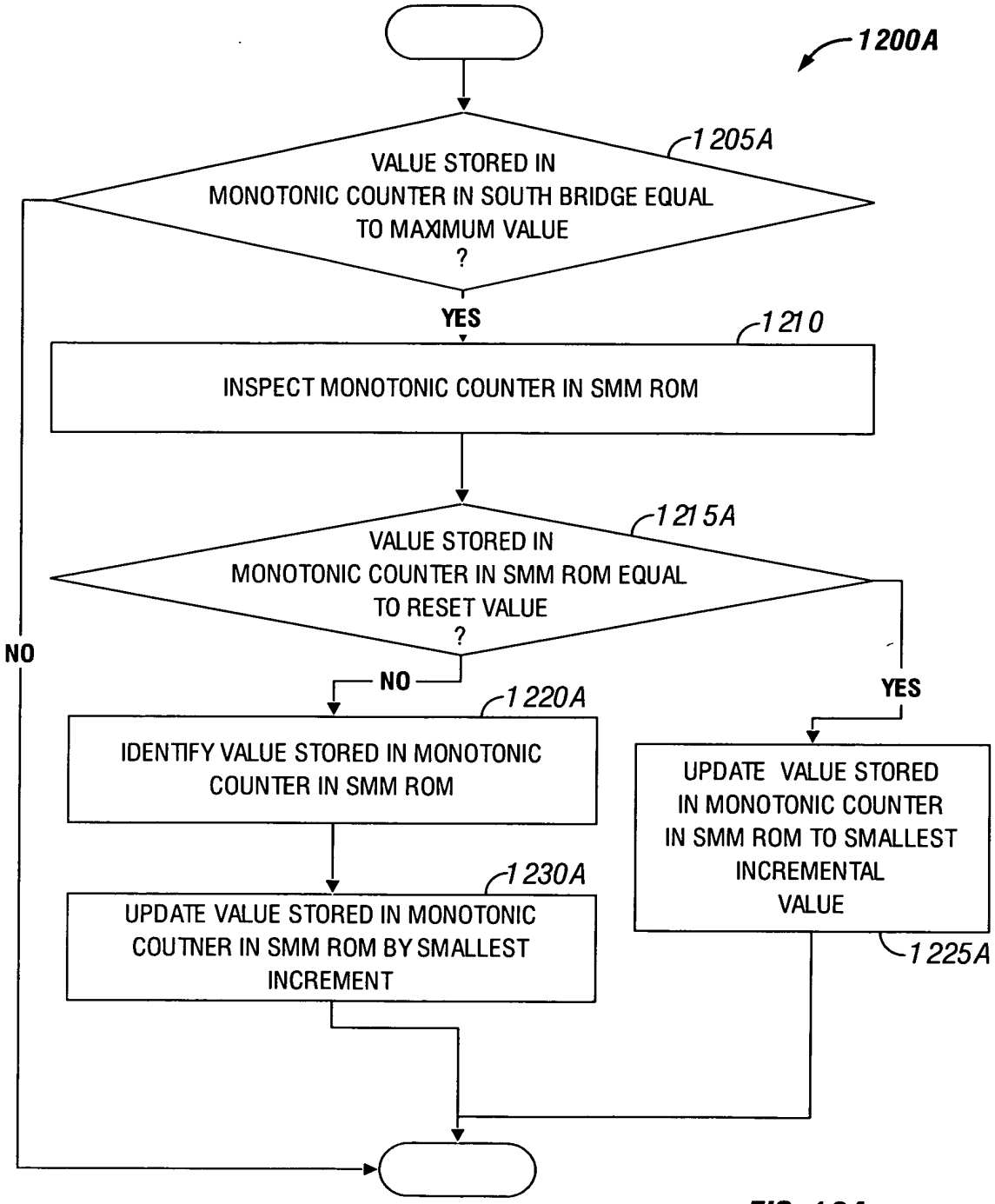
1200A
1205A
VALUE STORED IN MONOTONIC COUNTER IN SOUTH BRIDGE EQUAL TO MAXIMUM VALUE ?
YES
NO
1210
INSPECT MONOTONIC COUNTER IN SMM ROM
1215A
VALUE STORED IN MONOTONIC COUNTER IN SMM ROM EQUAL TO RESET VALUE ?
NO
YES
1220A
IDENTIFY VALUE STORED IN MONOTONIC COUNTER IN SMM ROM
1230A
UPDATE VALUE STORED IN MONOTONIC COUTNER IN SMM ROM BY SMALLEST INCREMENT
UPDATE VALUE STORED IN MONOTONIC COUNTER IN SMM ROM TO SMALLEST INCREMENTAL VALUE
1225A

FIG. 12A

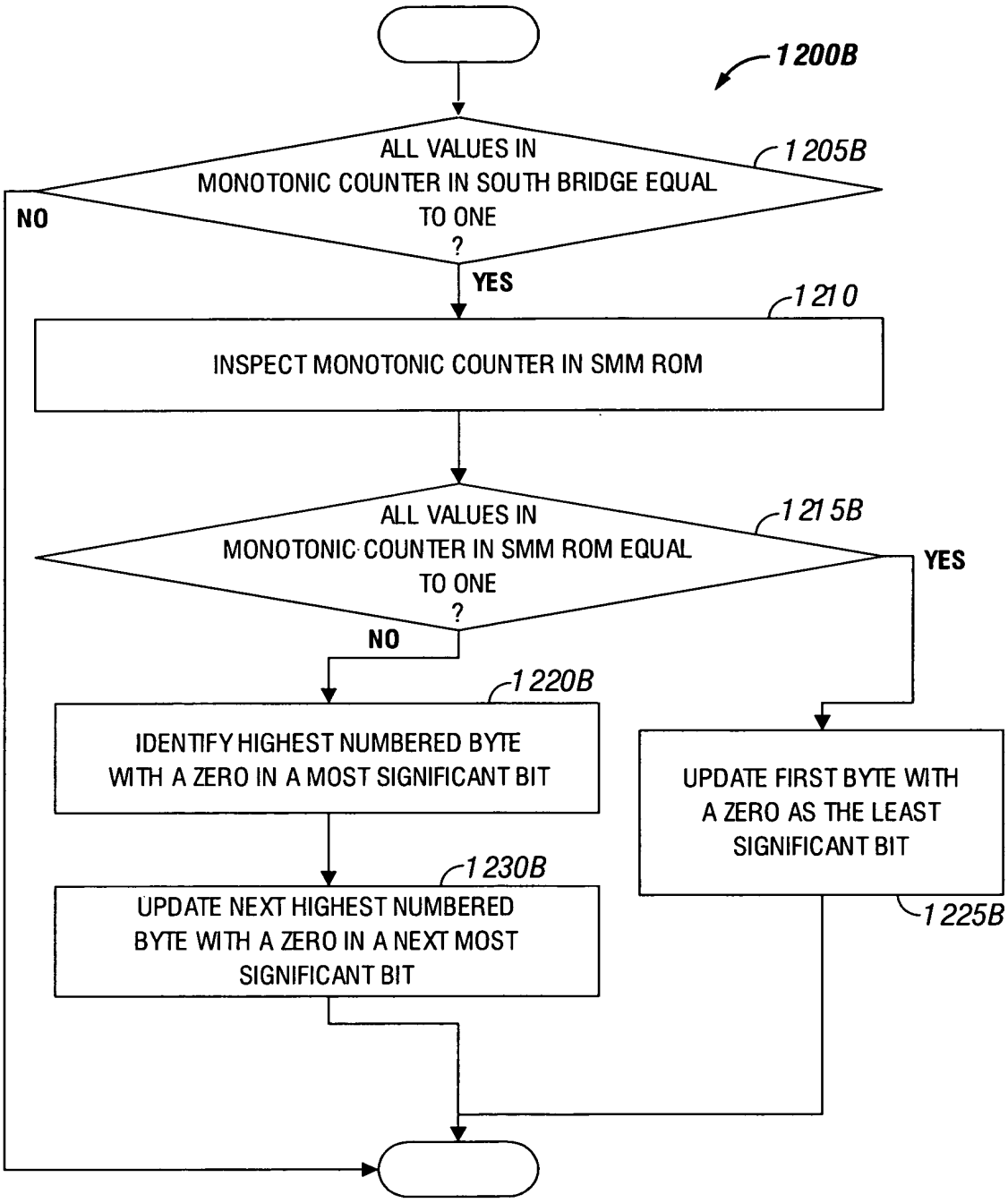
1200B
ALL VALUES IN MONOTONIC COUNTER IN SOUTH BRIDGE EQUAL TO ONE ?
1205B
NO
YES
1210
INSPECT MONOTONIC COUNTER IN SMM ROM
ALL VALUES IN MONOTONIC COUNTER IN SMM ROM EQUAL TO ONE ?
1215B
YES
NO
1220B
IDENTIFY HIGHEST NUMBERED BYTE WITH A ZERO IN A MOST SIGNIFICANT BIT
1230B
UPDATE NEXT HIGHEST NUMBERED BYTE WITH A ZERO IN A NEXT MOST SIGNIFICANT BIT
UPDATE FIRST BYTE WITH A ZERO AS THE LEAST SIGNIFICANT BIT
1225B

FIG. 12B

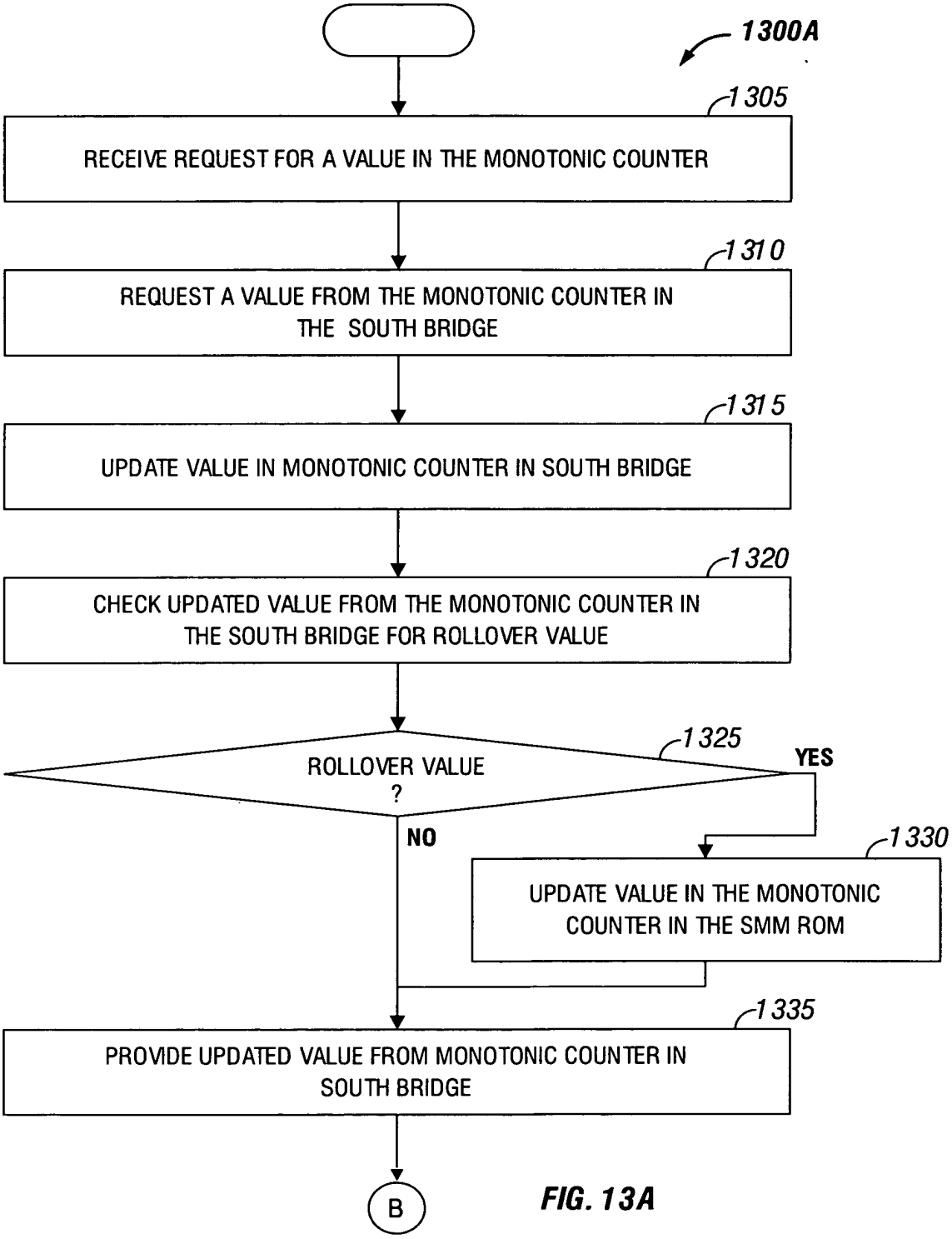
1300A
1305
RECEIVE REQUEST FOR A VALUE IN THE MONOTONIC COUNTER
1310
REQUEST A VALUE FROM THE MONOTONIC COUNTER IN THE SOUTH BRIDGE
1315
UPDATE VALUE IN MONOTONIC COUNTER IN SOUTH BRIDGE
1320
CHECK UPDATED VALUE FROM THE MONOTONIC COUNTER IN THE SOUTH BRIDGE FOR ROLLOVER VALUE
1325
ROLLOVER VALUE ?
YES
NO
1330
UPDATE VALUE IN THE MONOTONIC COUNTER IN THE SMM ROM
1335
PROVIDE UPDATED VALUE FROM MONOTONIC COUNTER IN SOUTH BRIDGE
B

FIG. 13A

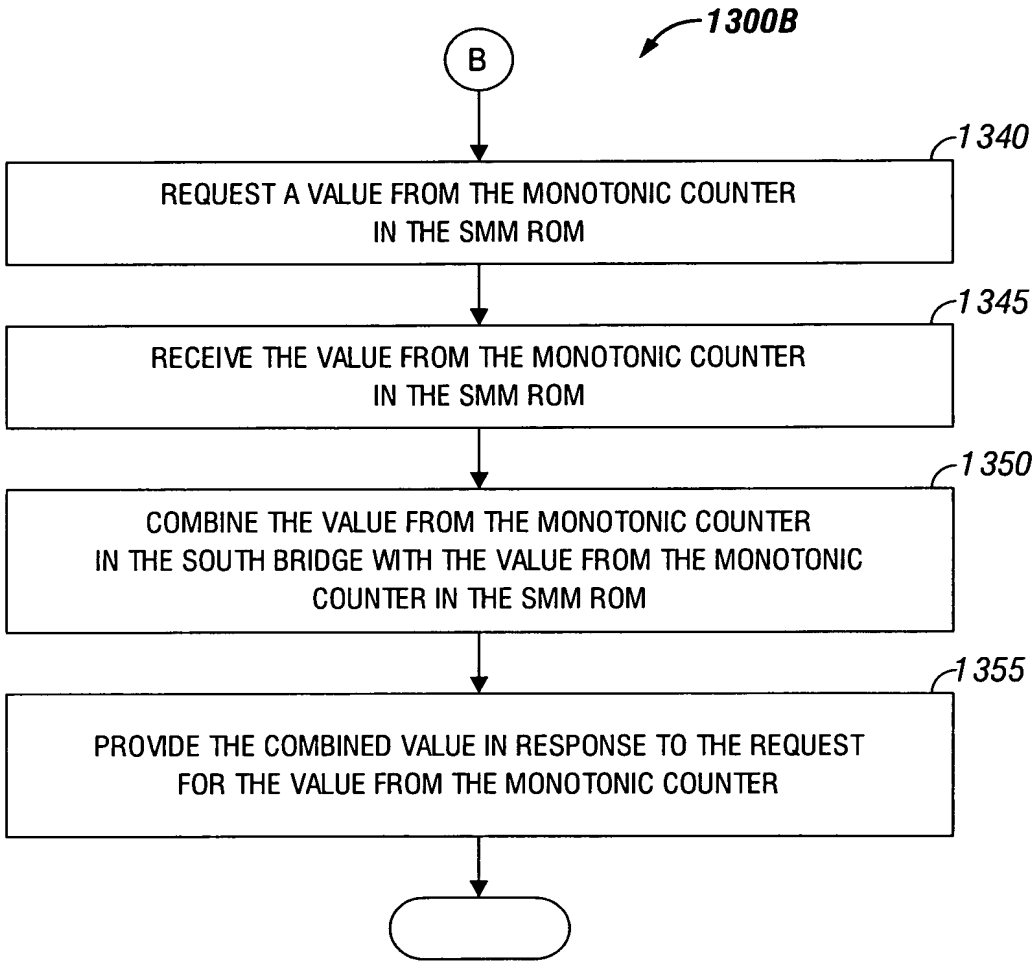
1300B
B
1340
REQUEST A VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM
1345
RECEIVE THE VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM
1350
COMBINE THE VALUE FROM THE MONOTONIC COUNTER IN THE SOUTH BRIDGE WITH THE VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM
1355
PROVIDE THE COMBINED VALUE IN RESPONSE TO THE REQUEST FOR THE VALUE FROM THE MONOTONIC COUNTER

FIG. 13B

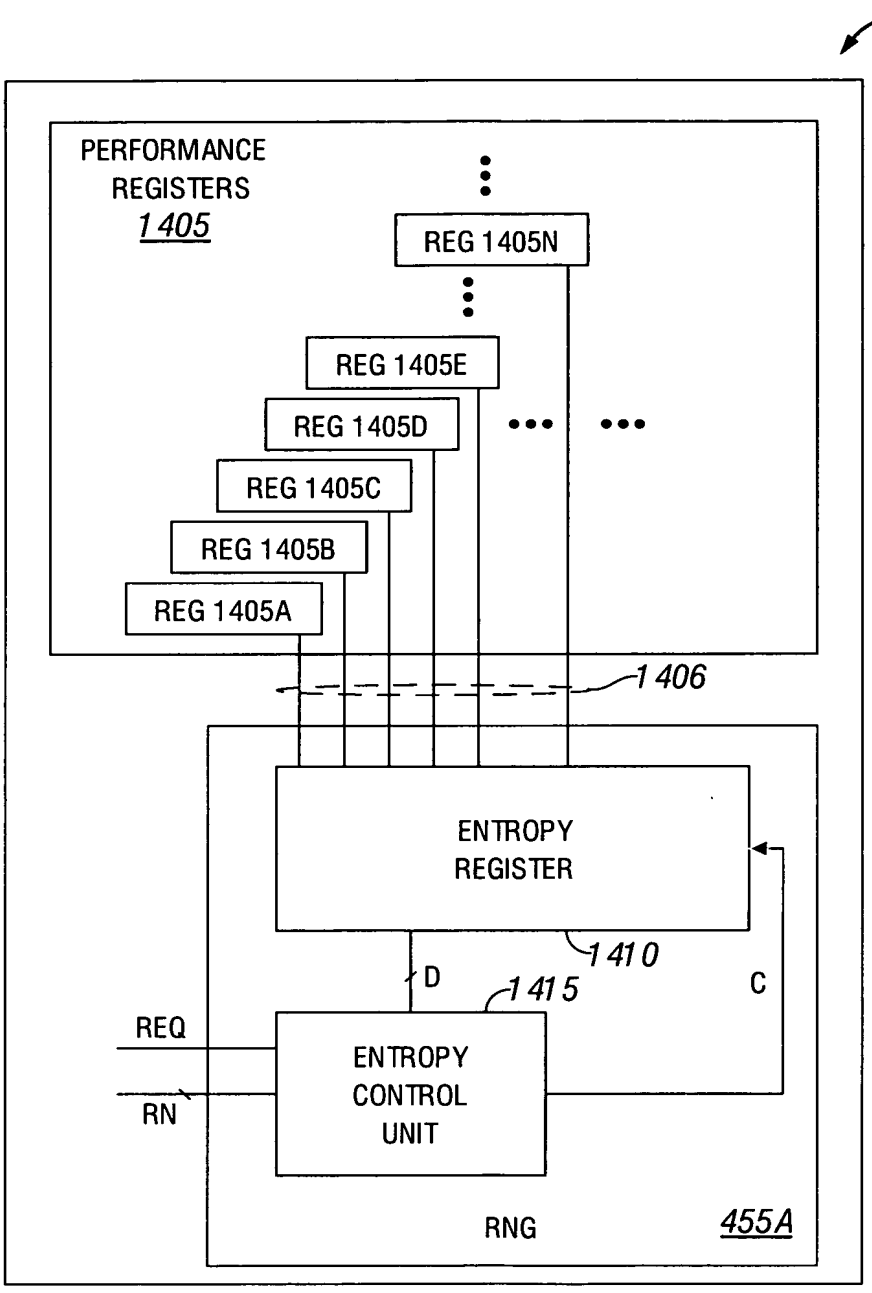
805A
PERFORMANCE REGISTERS
1405
REG 1405N
REG 1405E
REG 1405D
REG 1405C
REG 1405B
REG 1405A
1406
ENTROPY REGISTER
1410
D
1415
C
REQ
RN
ENTROPY CONTROL UNIT
RNG
455A

FIG. 14A

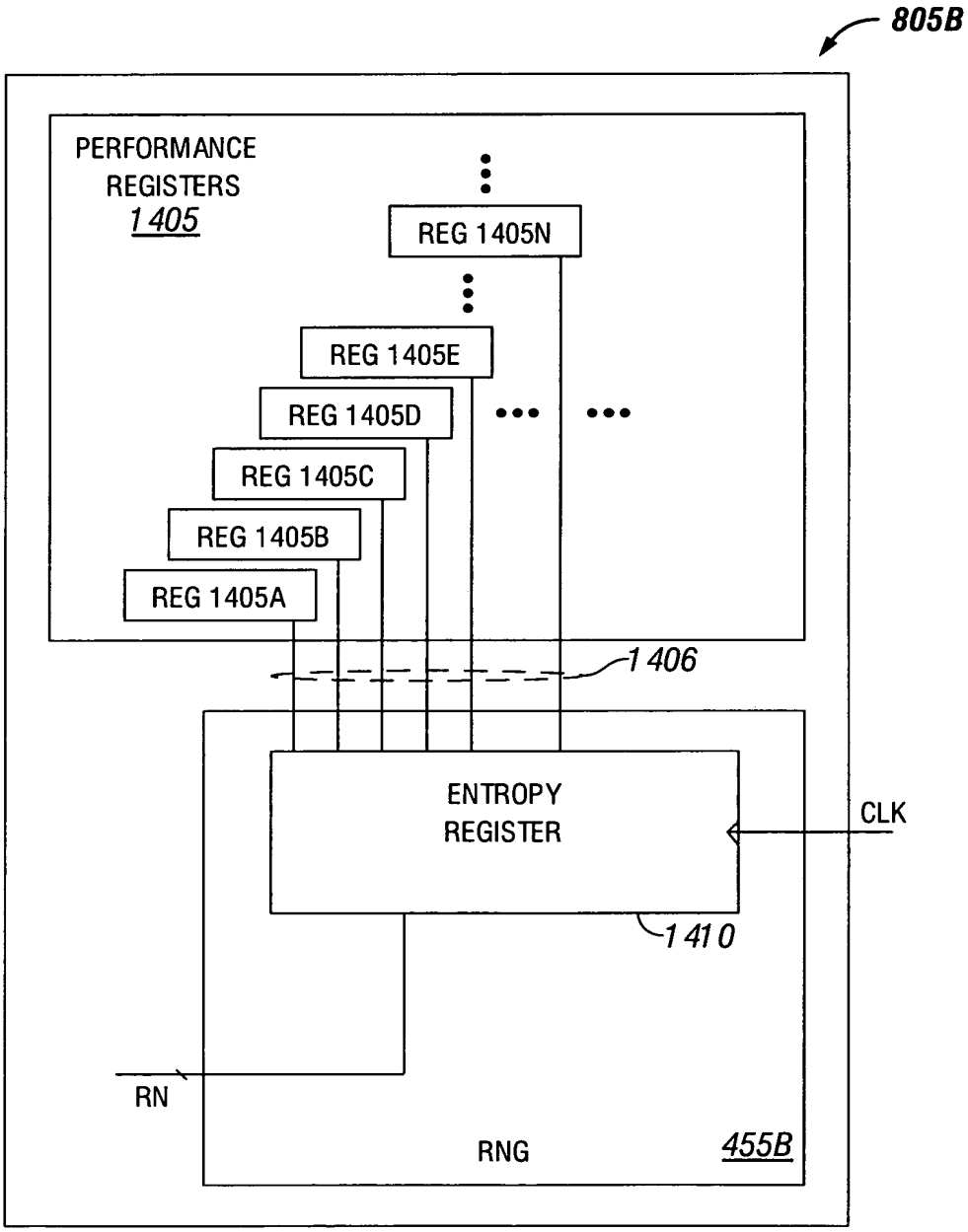
805B
PERFORMANCE
REGISTERS
1405
REG 1405N
REG 1405E
REG 1405D
REG 1405C
REG 1405B
REG 1405A
1406
ENTROPY
REGISTER
CLK
1410
RN
RNG
455B

FIG. 14B

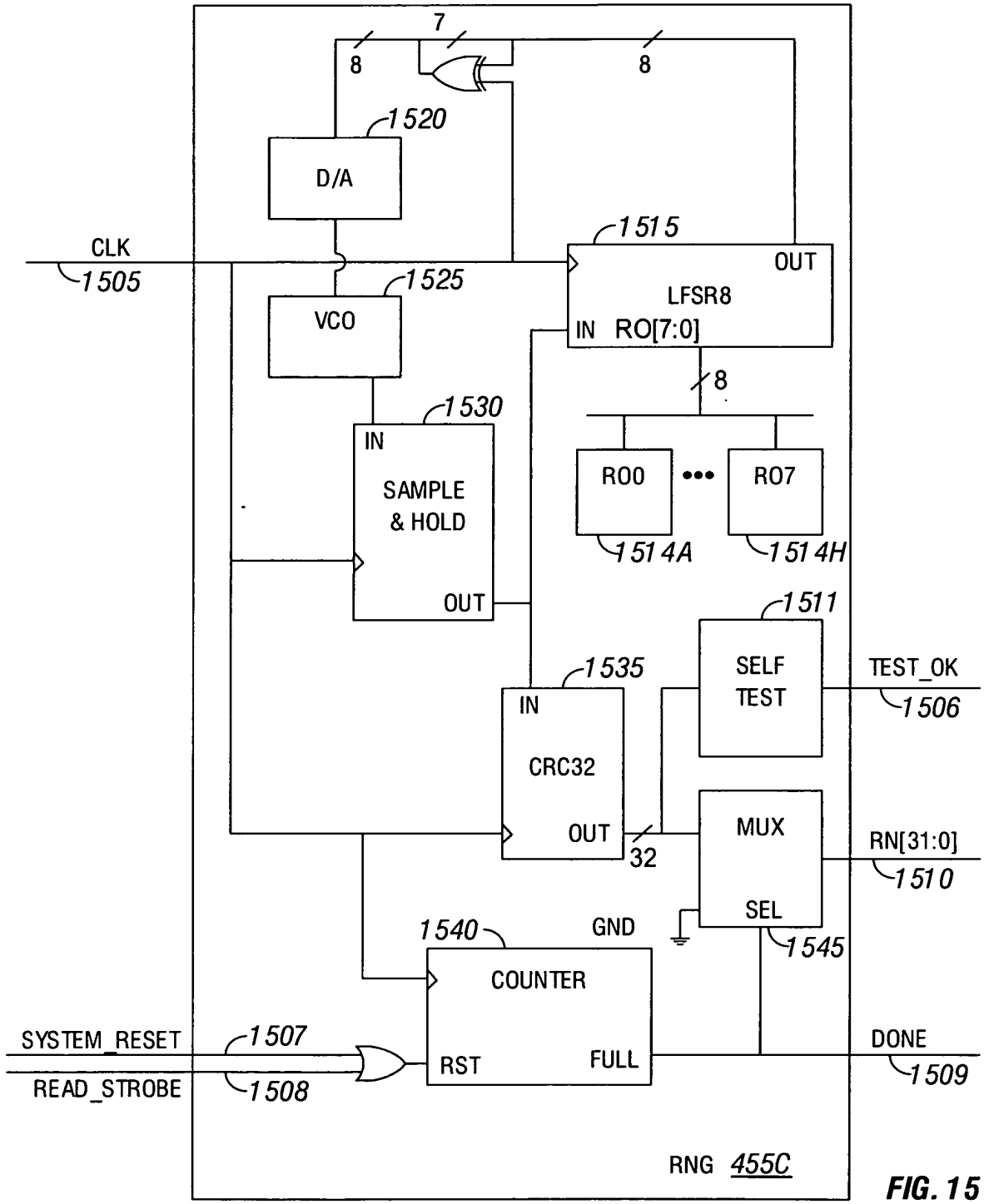
7
8
8
1520
D/A
CLK
1505
1515
OUT
LFSR8
IN RO[7:0]
1525
VCO
8
1530
IN
SAMPLE
& HOLD
OUT
RO0
RO7
1514A
1514H
1511
SELF
TEST
TEST_OK
1506
1535
IN
CRC32
OUT
32
MUX
RN[31:0]
1510
SEL
1545
1540
GND
COUNTER
SYSTEM_RESET
1507
READ_STROBE
1508
RST
FULL
DONE
1509
RNG 455C

FIG. 15

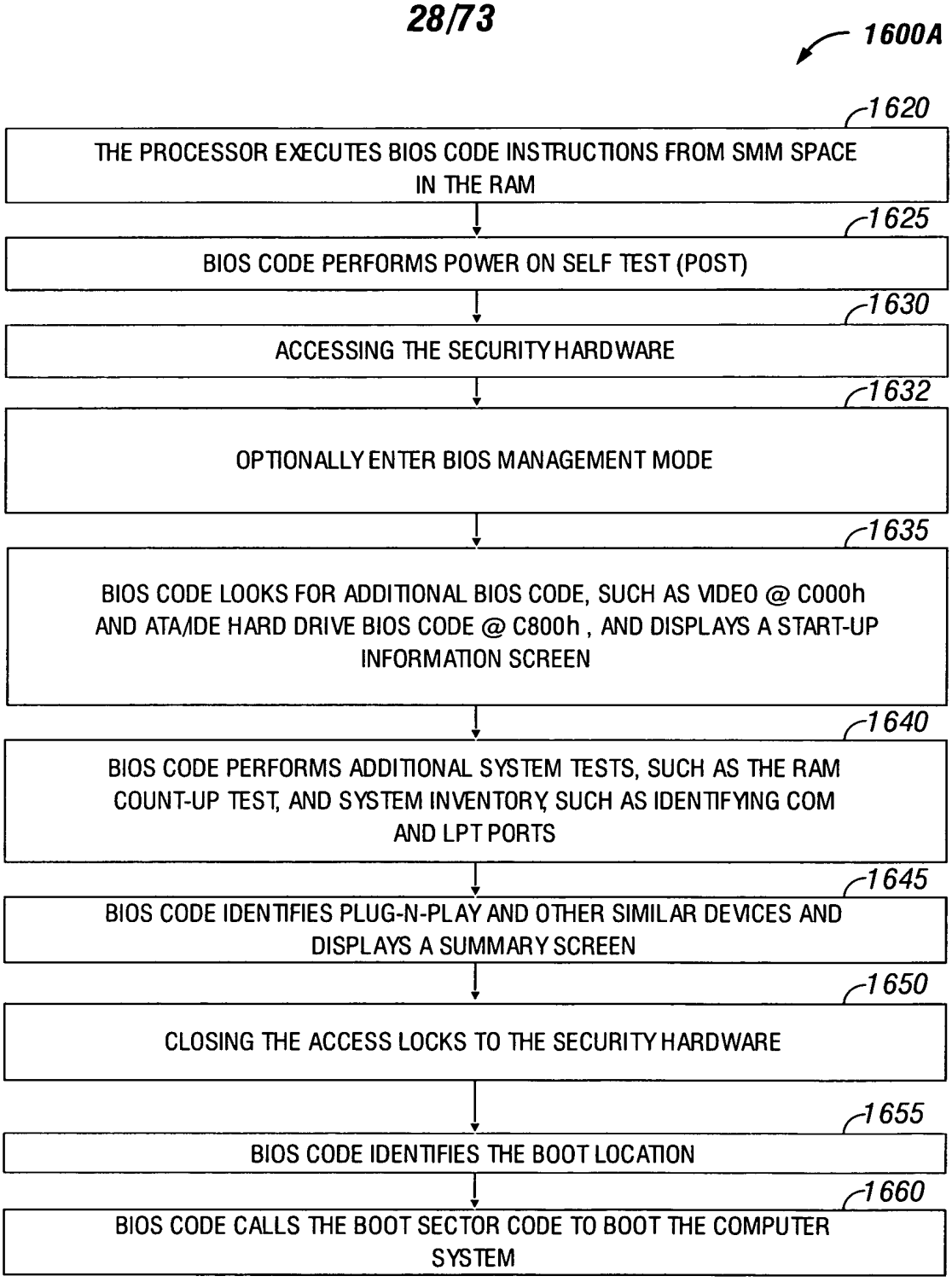
1600A
1620
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM
1625
BIOS CODE PERFORMS POWER ON SELF TEST (POST)
1630
ACCESSING THE SECURITY HARDWARE
1632
OPTIONALLY ENTER BIOS MANAGEMENT MODE
1635
BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h , AND DISPLAYS A START-UP INFORMATION SCREEN
1640
BIOS CODE PERFORMS ADDITIONAL SYSTEM TESTS, SUCH AS THE RAM COUNT-UP TEST, AND SYSTEM INVENTORY, SUCH AS IDENTIFYING COM AND LPT PORTS
1645
BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN
1650
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE
1655
BIOS CODE IDENTIFIES THE BOOT LOCATION
1660
BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM

FIG. 16A

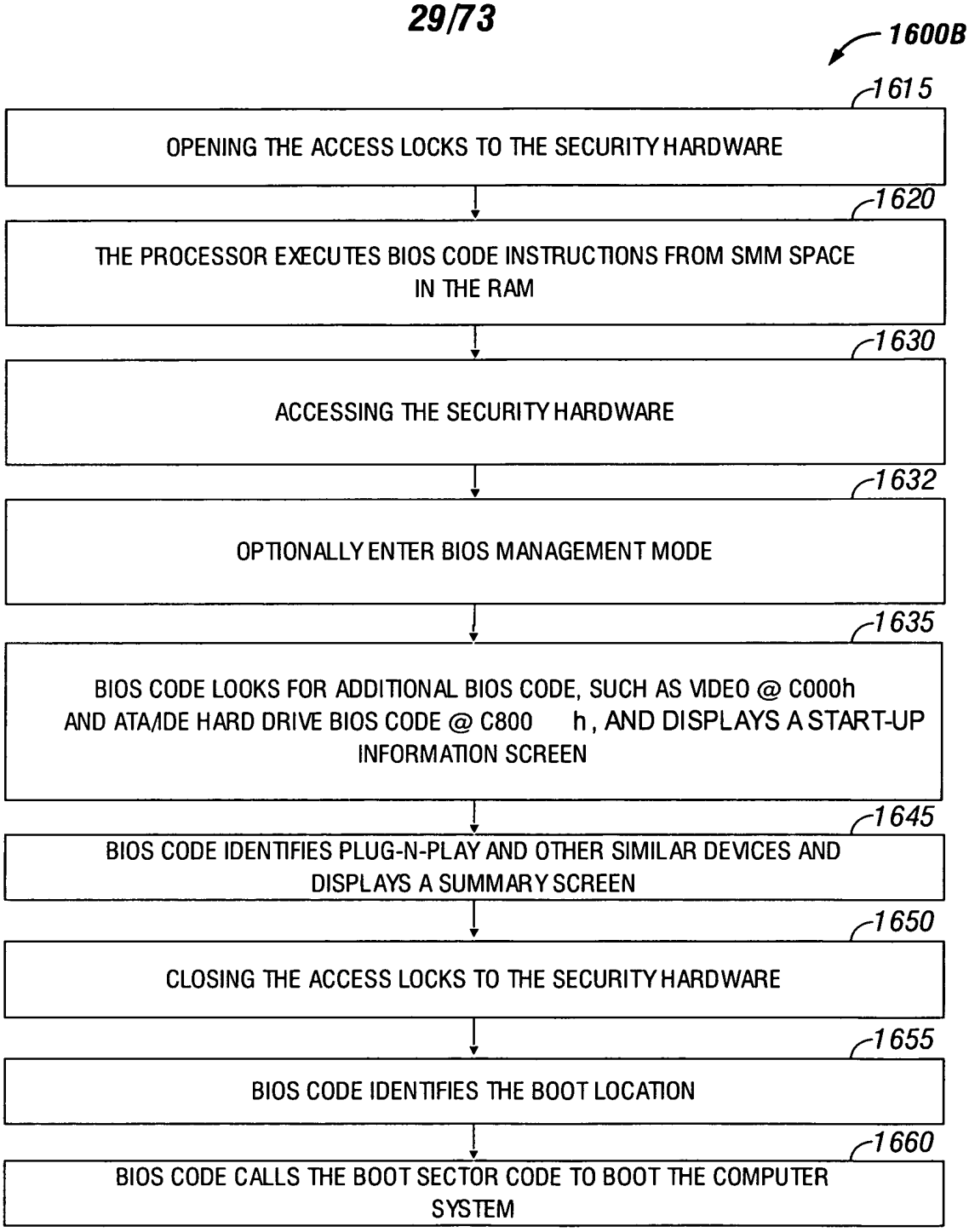
1600B
1615
OPENING THE ACCESS LOCKS TO THE SECURITY HARDWARE
1620
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM
1630
ACCESSING THE SECURITY HARDWARE
1632
OPTIONALLY ENTER BIOS MANAGEMENT MODE
1635
BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800 h, AND DISPLAYS A START-UP INFORMATION SCREEN
1645
BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN
1650
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE
1655
BIOS CODE IDENTIFIES THE BOOT LOCATION
1660
BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM

FIG. 16B

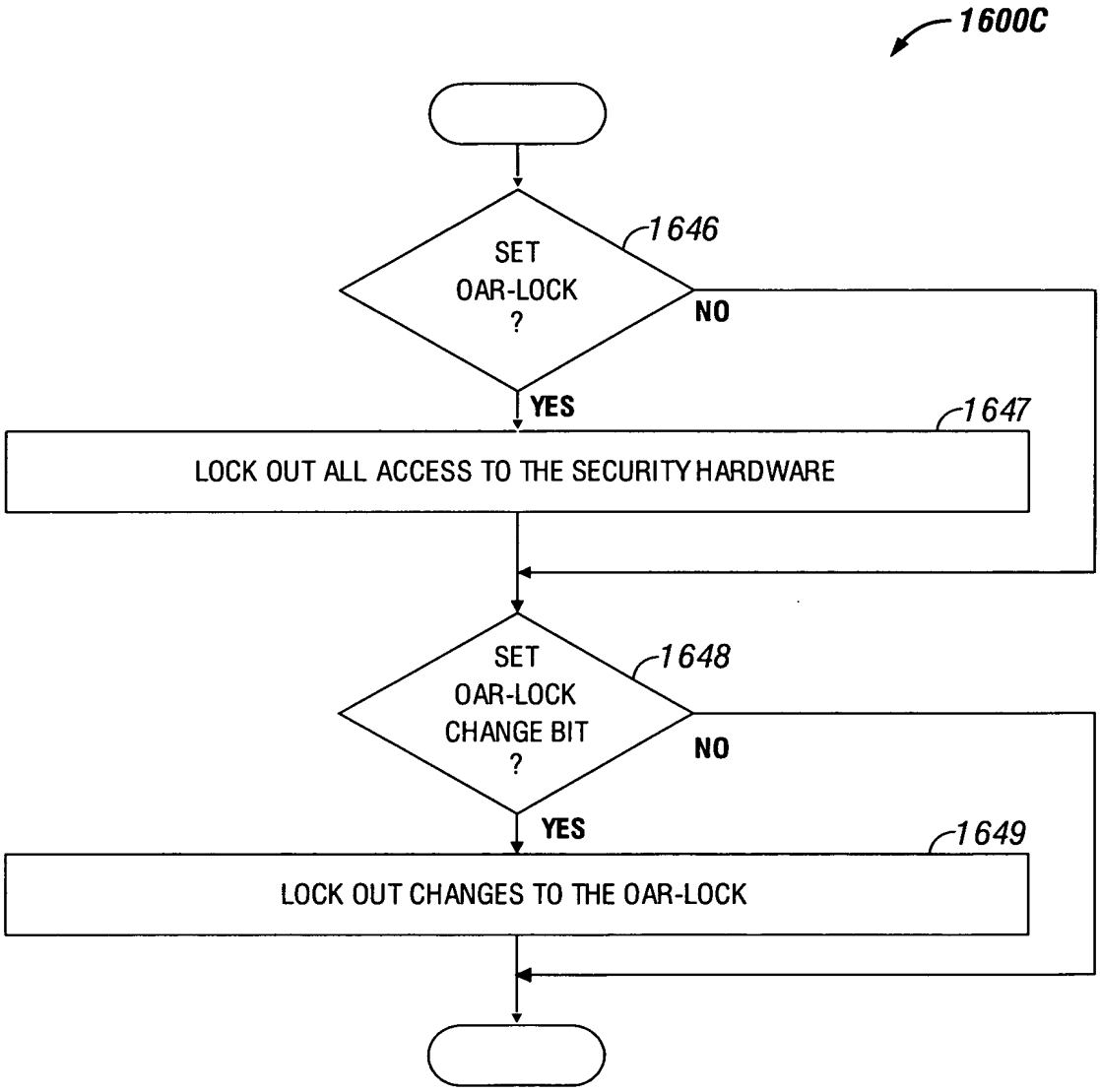
1600C
SET OAR-LOCK ?
1646
NO
YES
1647
LOCK OUT ALL ACCESS TO THE SECURITY HARDWARE
SET OAR-LOCK CHANGE BIT ?
1648
NO
YES
1649
LOCK OUT CHANGES TO THE OAR-LOCK

Fig. 16C

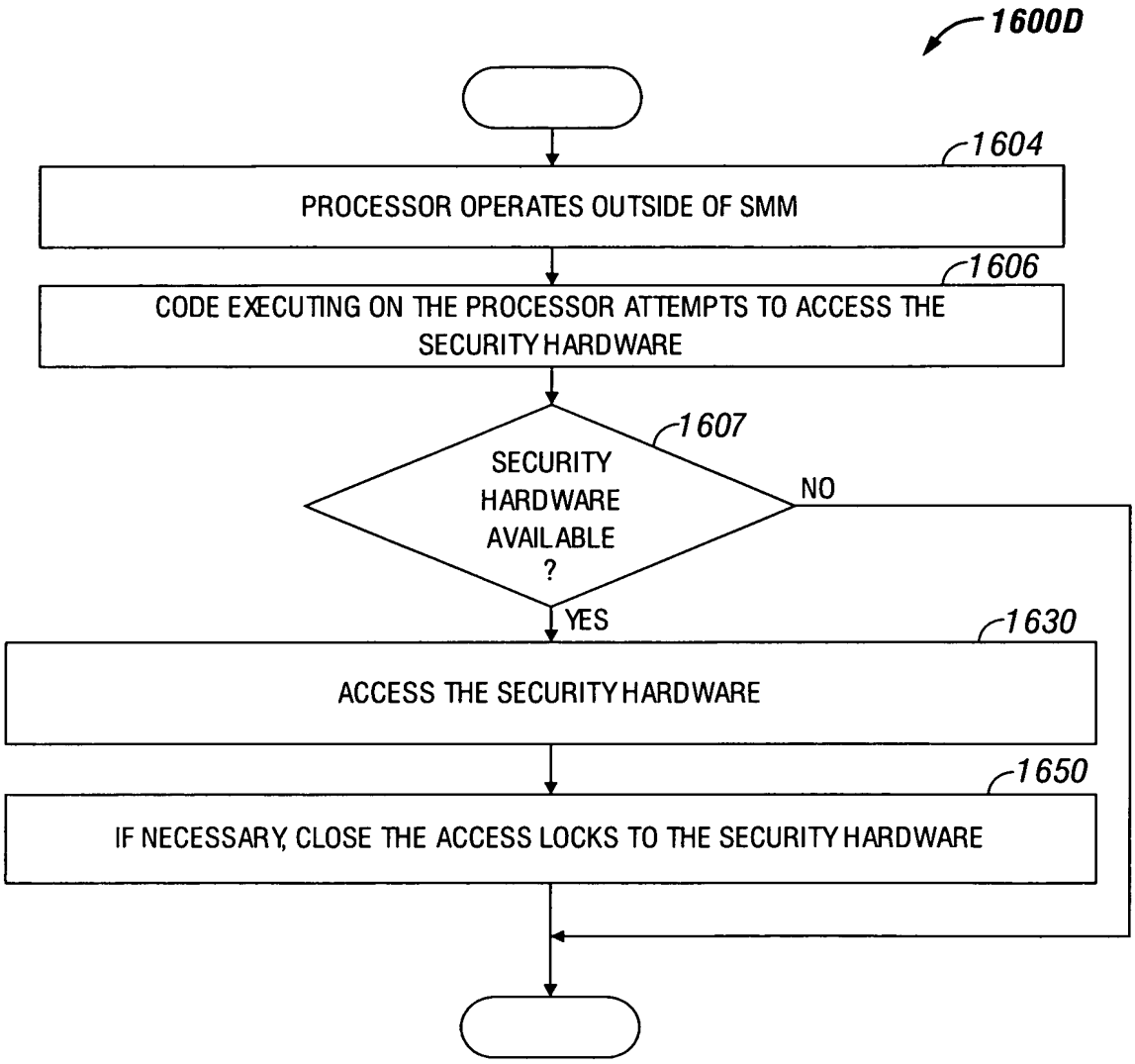
1600D
1604
PROCESSOR OPERATES OUTSIDE OF SMM
1606
CODE EXECUTING ON THE PROCESSOR ATTEMPTS TO ACCESS THE SECURITY HARDWARE
1607
SECURITY HARDWARE AVAILABLE ?
NO
YES
1630
ACCESS THE SECURITY HARDWARE
1650
IF NECESSARY, CLOSE THE ACCESS LOCKS TO THE SECURITY HARDWARE

FIG. 16D

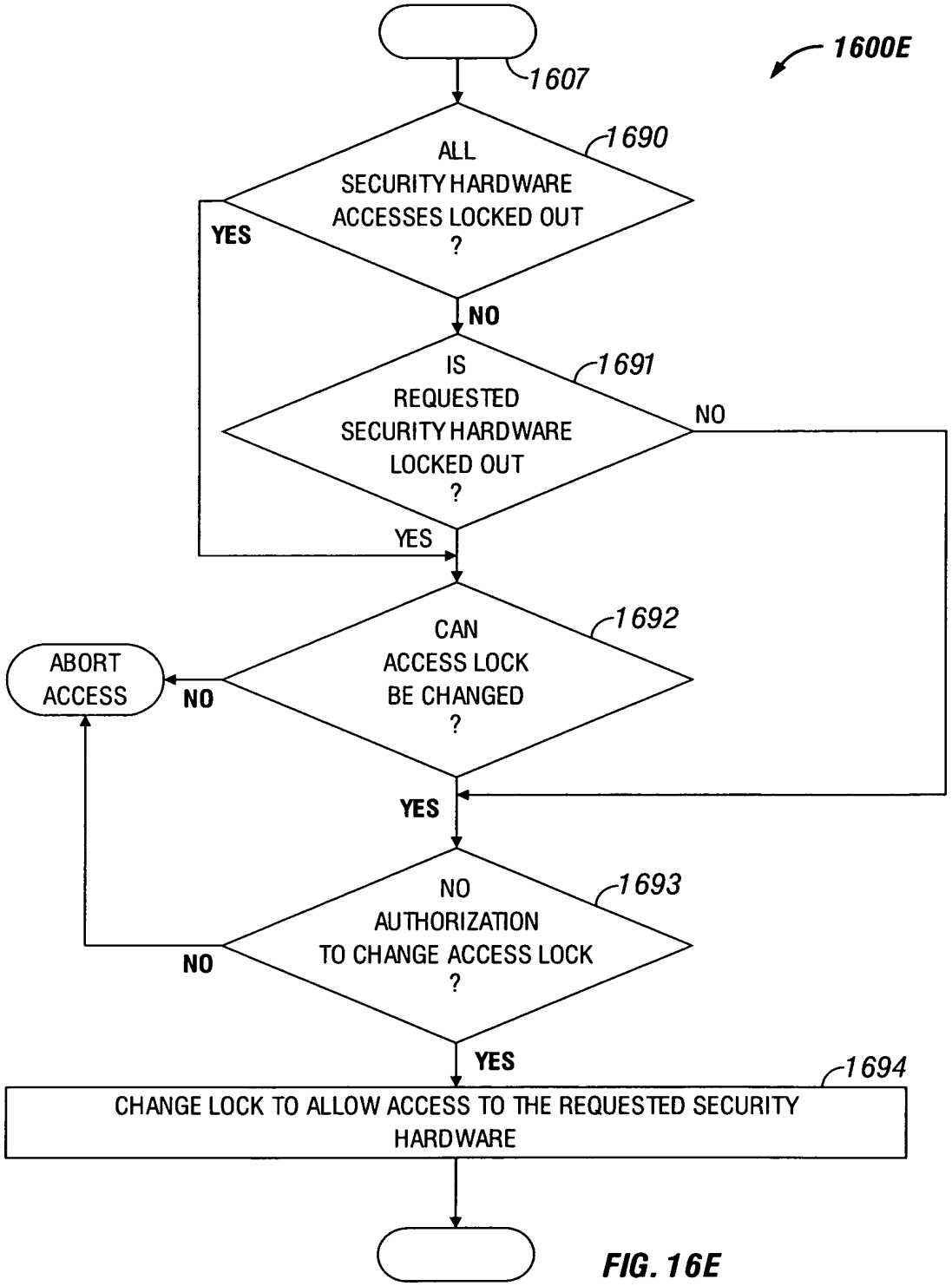
1600E
1607
1690
ALL SECURITY HARDWARE ACCESSES LOCKED OUT ?
YES
NO
1691
IS REQUESTED SECURITY HARDWARE LOCKED OUT ?
NO
YES
1692
CAN ACCESS LOCK BE CHANGED ?
ABORT ACCESS
NO
YES
1693
NO AUTHORIZATION TO CHANGE ACCESS LOCK ?
NO
YES
1694
CHANGE LOCK TO ALLOW ACCESS TO THE REQUESTED SECURITY HARDWARE

FIG. 16E

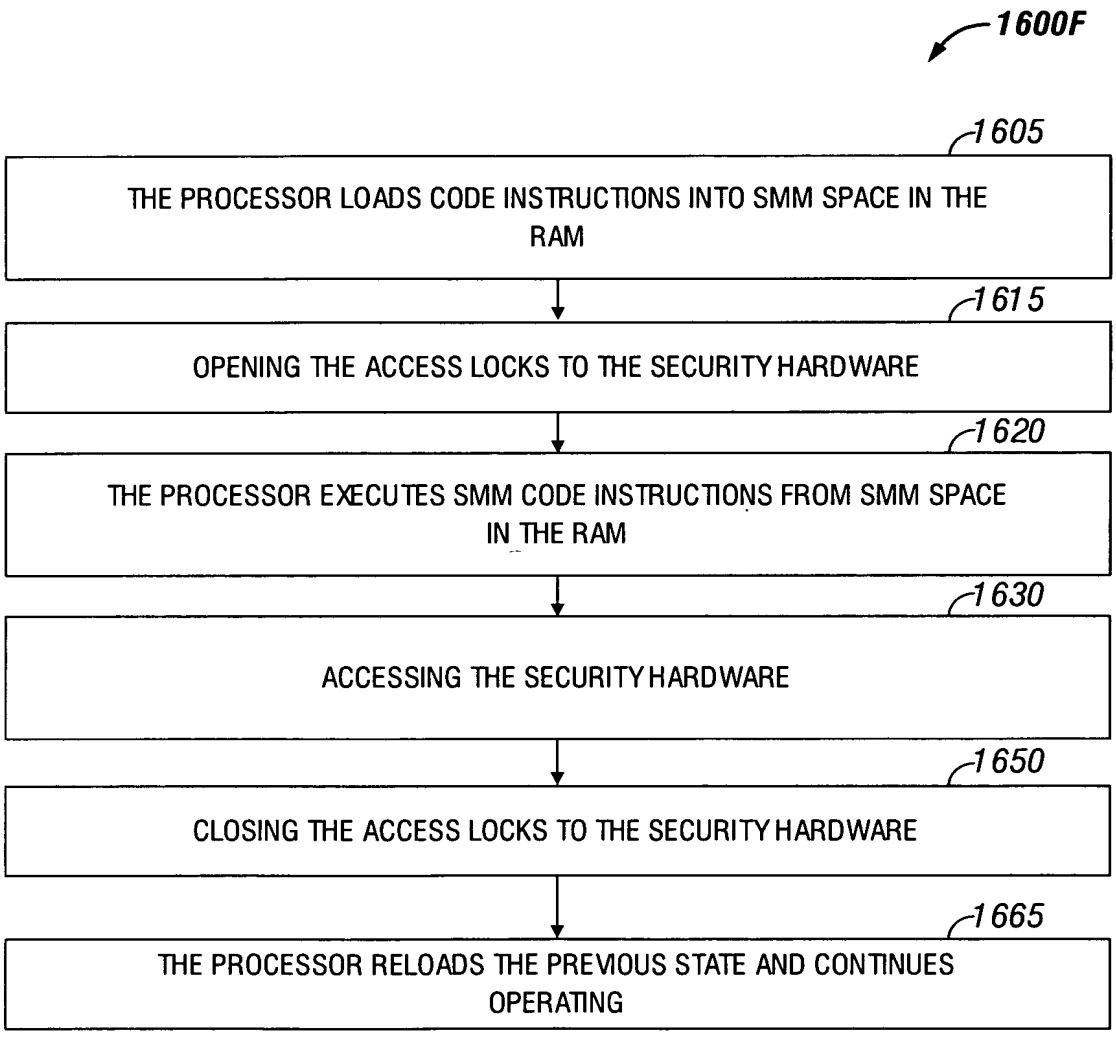
1600F
1605
THE PROCESSOR LOADS CODE INSTRUCTIONS INTO SMM SPACE IN THE RAM
1615
OPENING THE ACCESS LOCKS TO THE SECURITY HARDWARE
1620
THE PROCESSOR EXECUTES SMM CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM
1630
ACCESSING THE SECURITY HARDWARE
1650
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE
1665
THE PROCESSOR RELOADS THE PREVIOUS STATE AND CONTINUES OPERATING

FIG. 16F

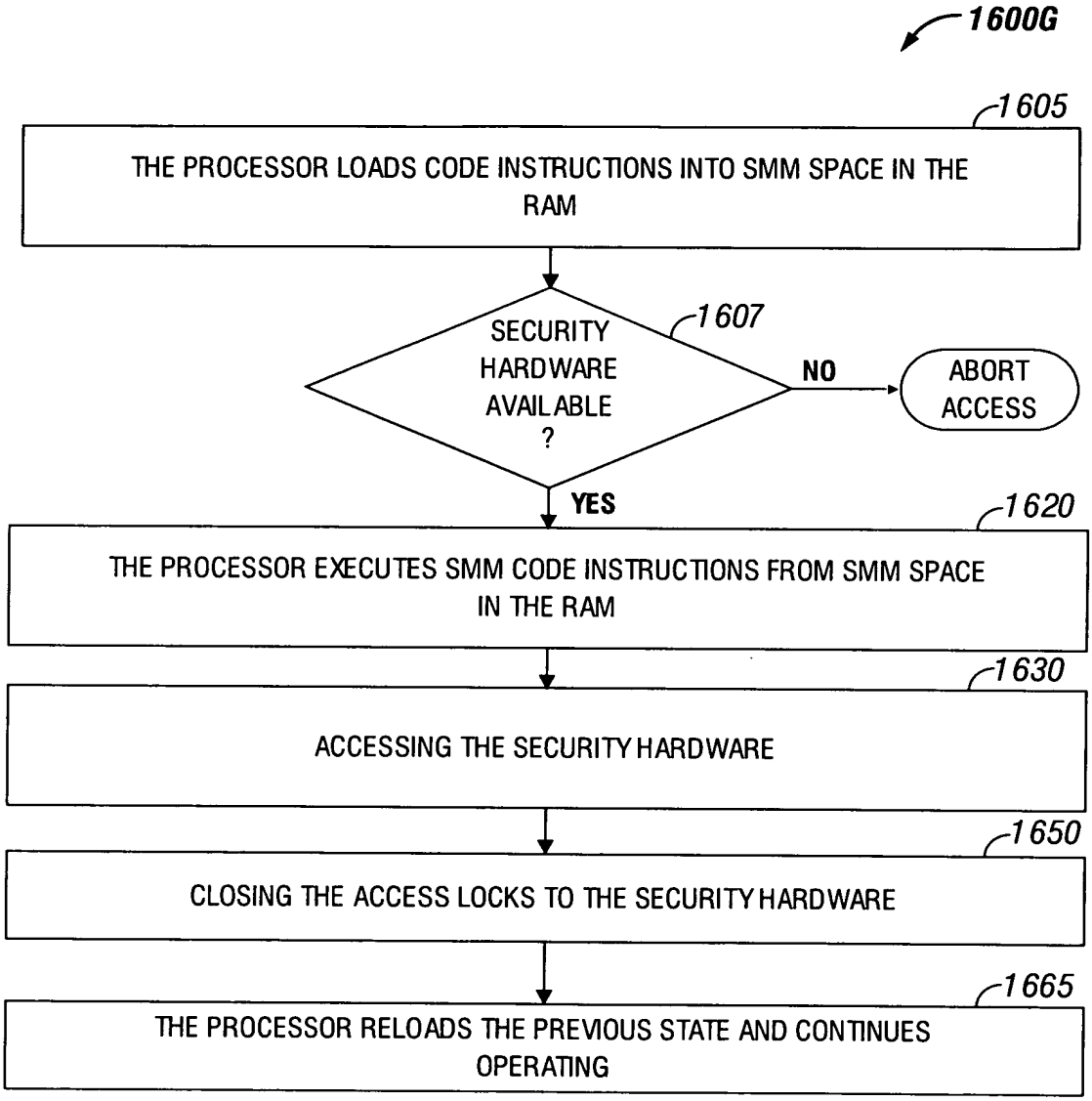
1600G
1605
THE PROCESSOR LOADS CODE INSTRUCTIONS INTO SMM SPACE IN THE RAM
1607
SECURITY HARDWARE AVAILABLE ?
NO
ABORT ACCESS
YES
1620
THE PROCESSOR EXECUTES SMM CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM
1630
ACCESSING THE SECURITY HARDWARE
1650
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE
1665
THE PROCESSOR RELOADS THE PREVIOUS STATE AND CONTINUES OPERATING

FIG. 16G

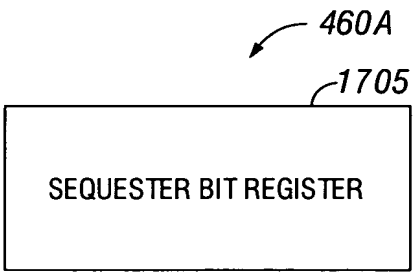

FIG. 17A

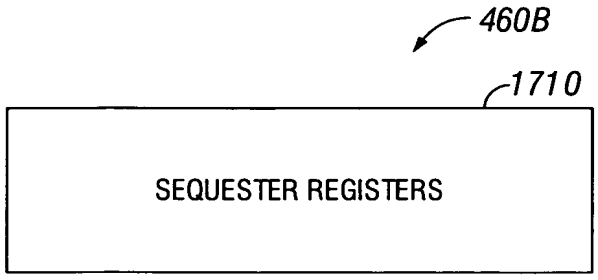

FIG. 17B

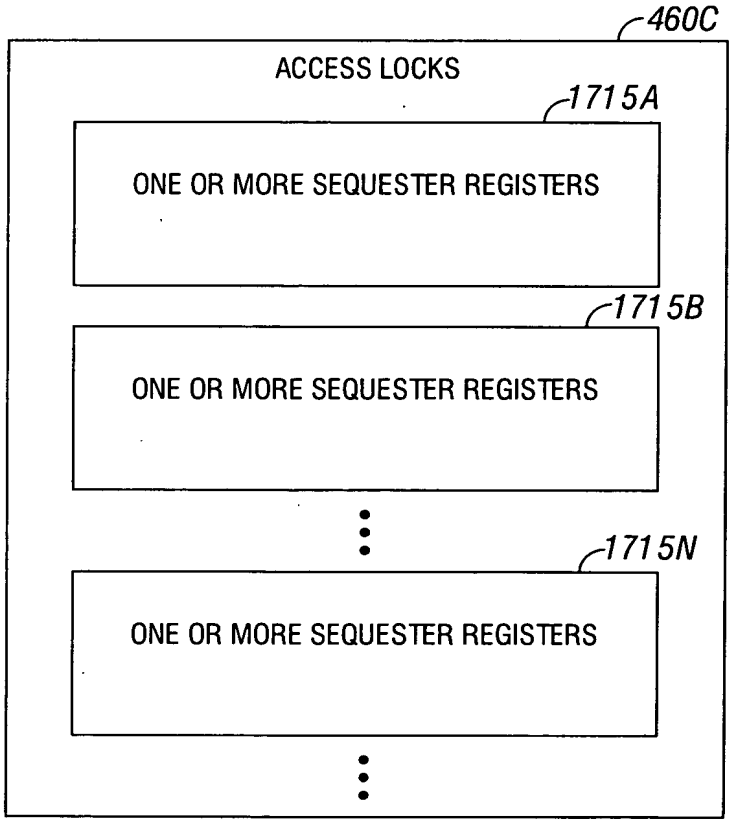

FIG. 17C

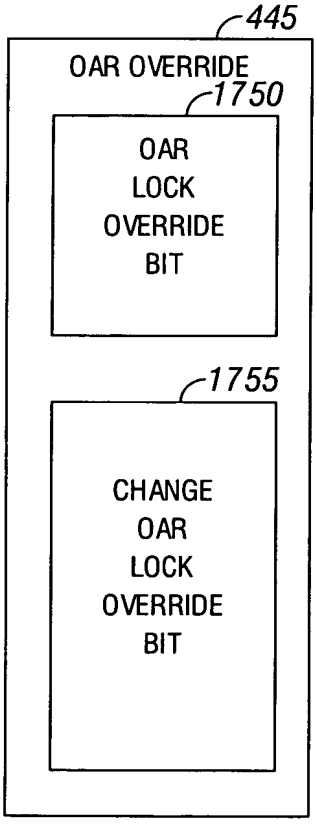

FIG. 17D

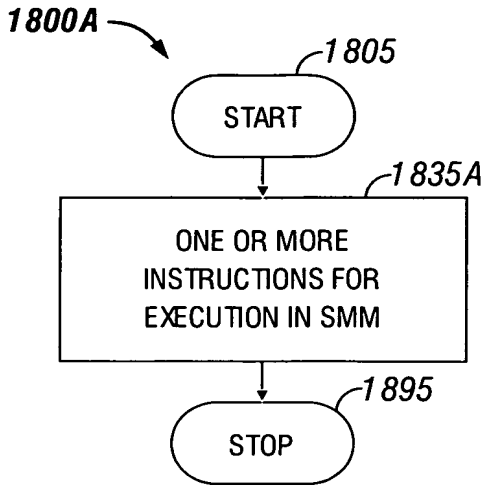

FIG. 18A
(Prior Art)

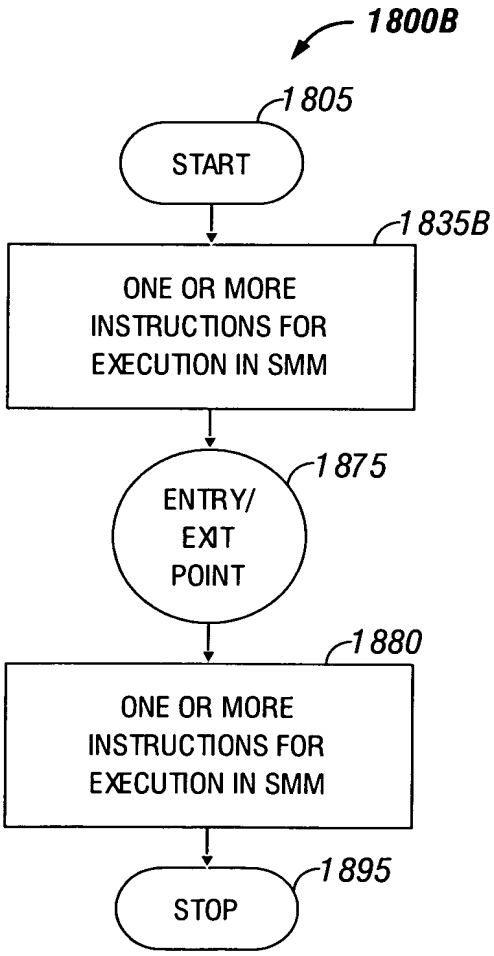

FIG. 18B

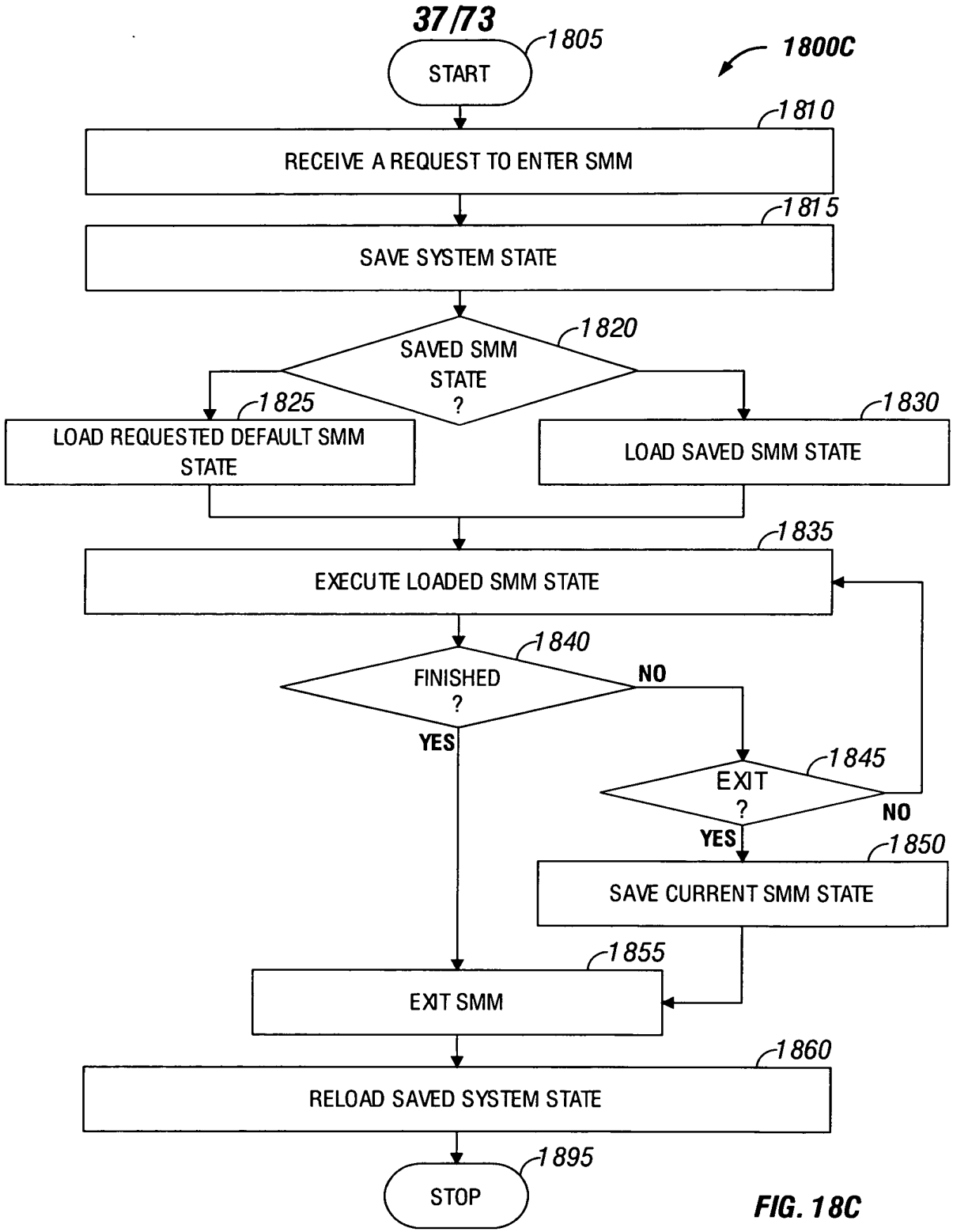
1800C
1805
START
1810
RECEIVE A REQUEST TO ENTER SMM
1815
SAVE SYSTEM STATE
1820
SAVED SMM STATE ?
1825
LOAD REQUESTED DEFAULT SMM STATE
1830
LOAD SAVED SMM STATE
1835
EXECUTE LOADED SMM STATE
1840
FINISHED ?
NO
YES
1845
EXIT ?
NO
YES
1850
SAVE CURRENT SMM STATE
1855
EXIT SMM
1860
RELOAD SAVED SYSTEM STATE
1895
STOP

FIG. 18C

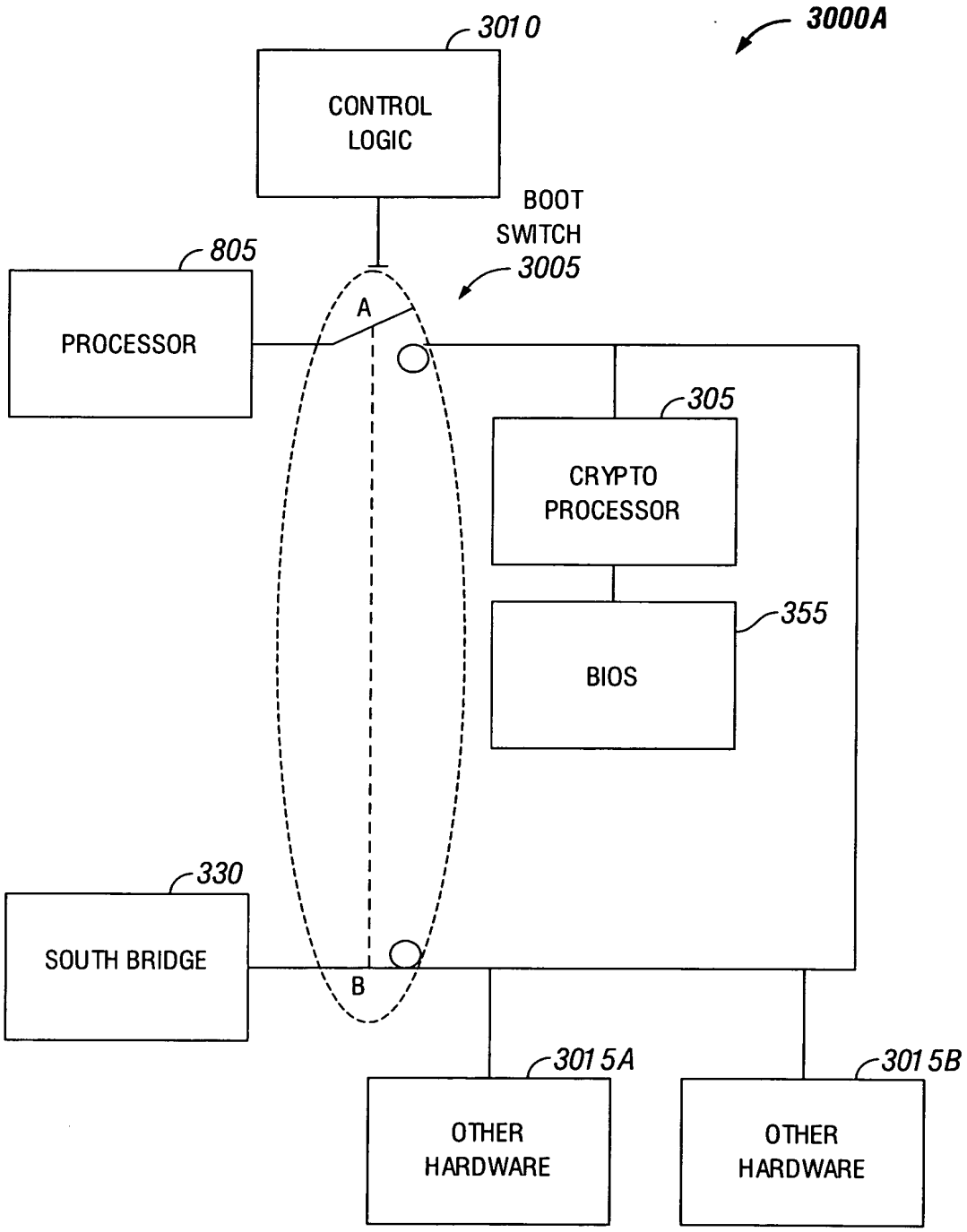
3010
3000A
CONTROL LOGIC
BOOT SWITCH
3005
805
PROCESSOR
A
305
CRYPTO PROCESSOR
355
BIOS
330
SOUTH BRIDGE
B
3015A
3015B
OTHER HARDWARE
OTHER HARDWARE

FIG. 19A

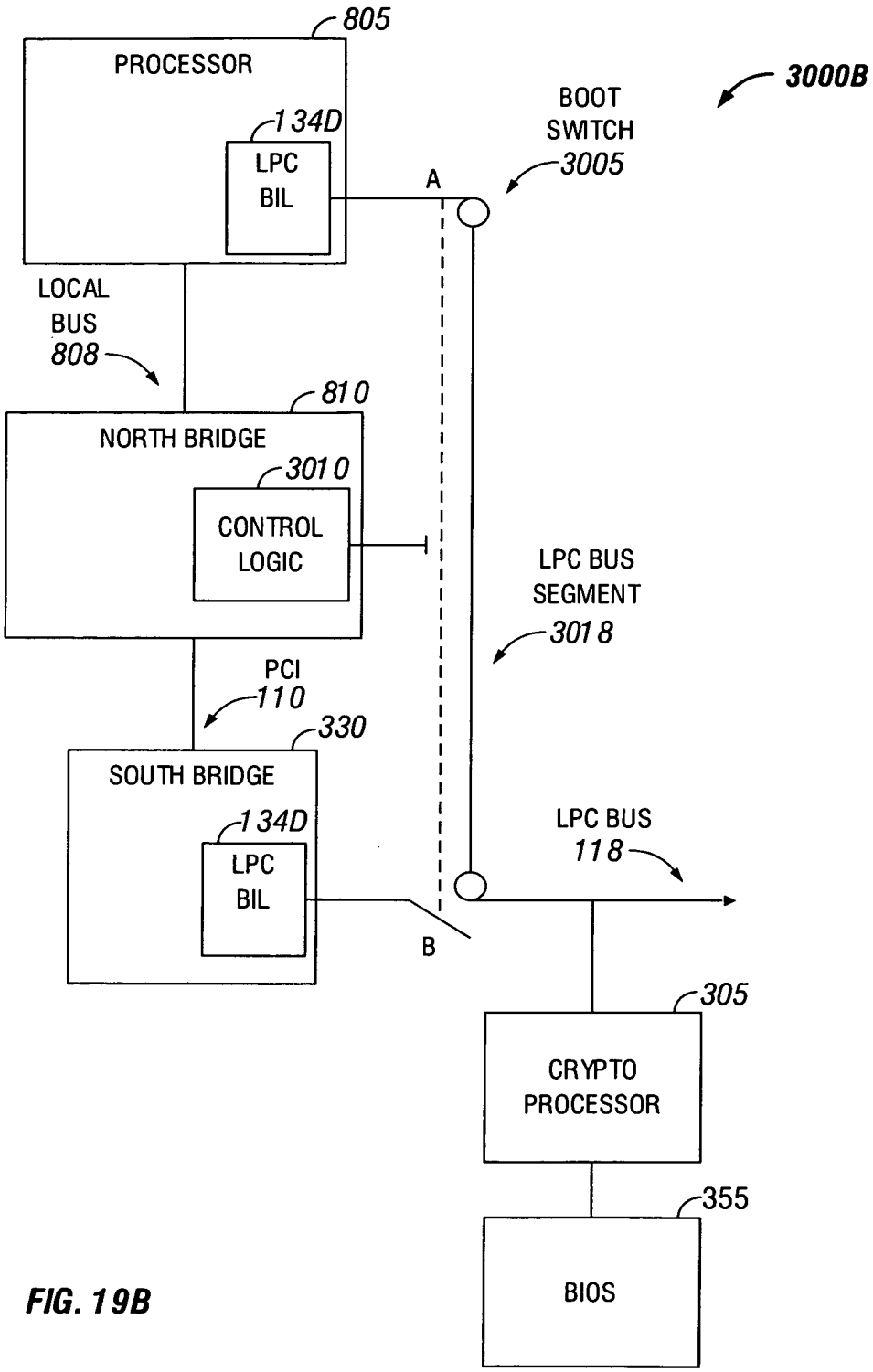
805
PROCESSOR
134D
LPC BIL
3000B
BOOT SWITCH
3005
A
LOCAL BUS
808
810
NORTH BRIDGE
3010
CONTROL LOGIC
LPC BUS SEGMENT
3018
PCI
110
330
SOUTH BRIDGE
134D
LPC BIL
LPC BUS
118
B
305
CRYPTO PROCESSOR
355
BIOS

FIG. 19B

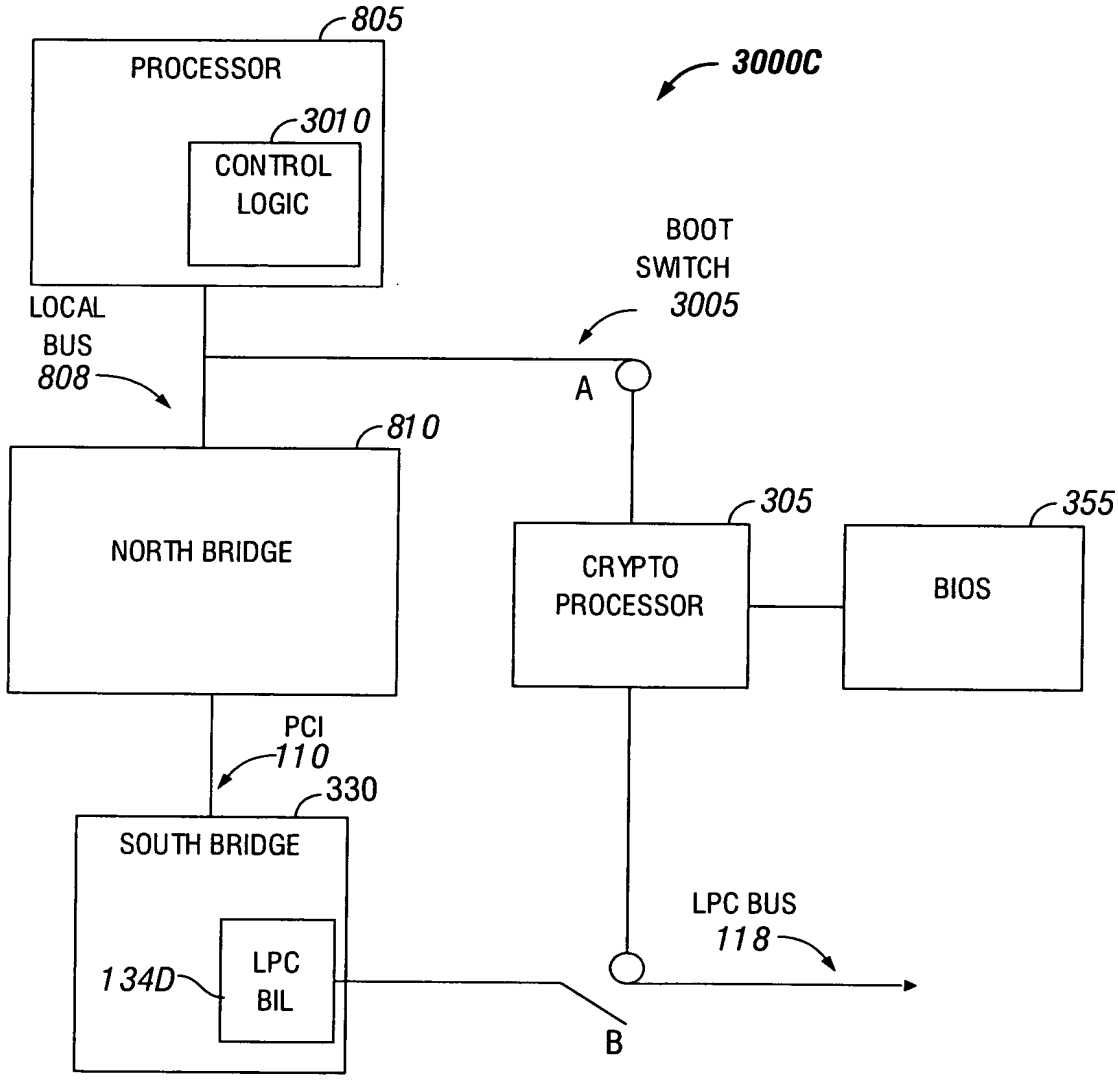
805
PROCESSOR
3010
CONTROL LOGIC
3000C
BOOT SWITCH
3005
LOCAL BUS
808
A
810
NORTH BRIDGE
305
CRYPTO PROCESSOR
355
BIOS
PCI
110
330
SOUTH BRIDGE
LPC BUS
118
134D
LPC BIL
B

FIG. 19C

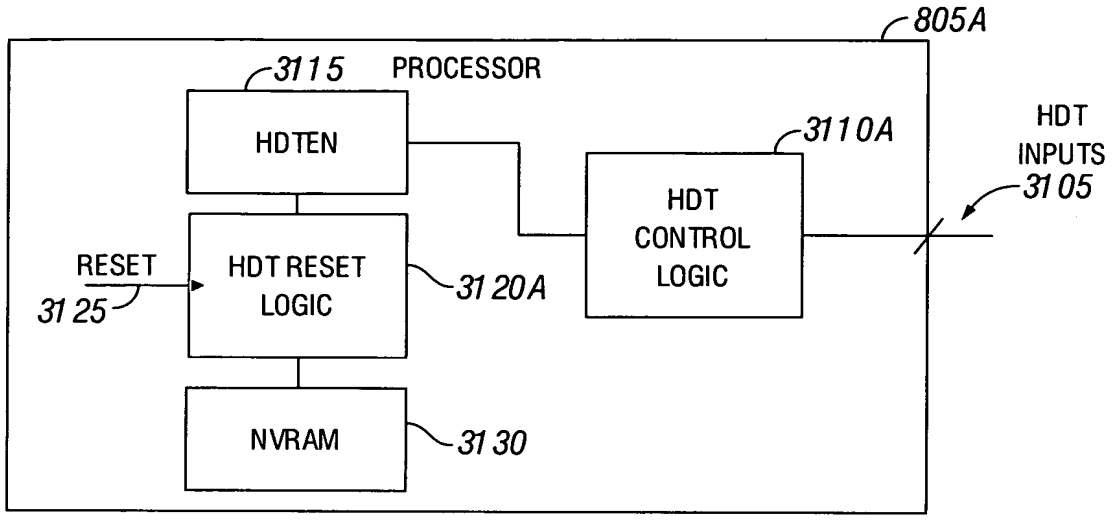

FIG. 20A

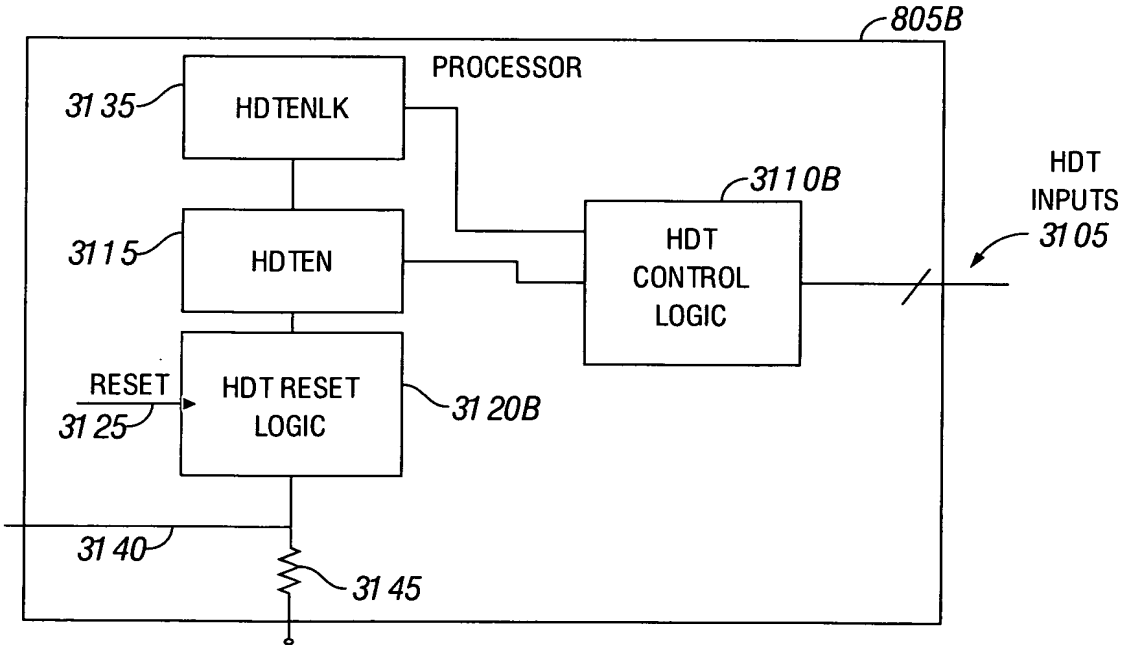

FIG. 20B

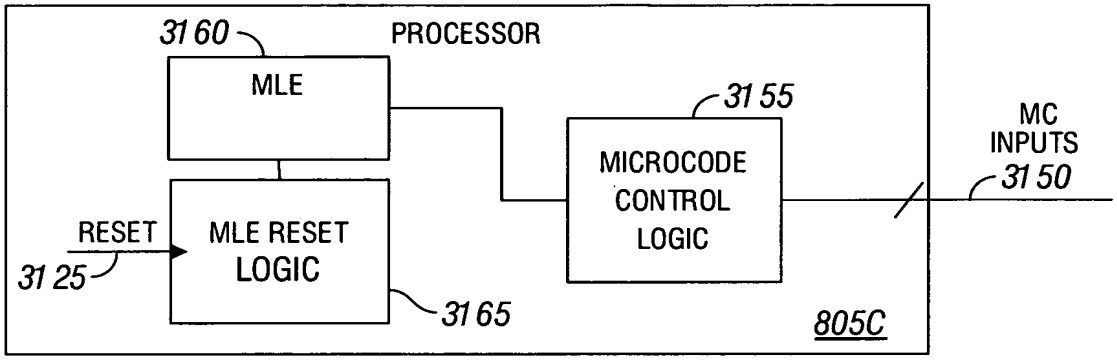

FIG. 20C

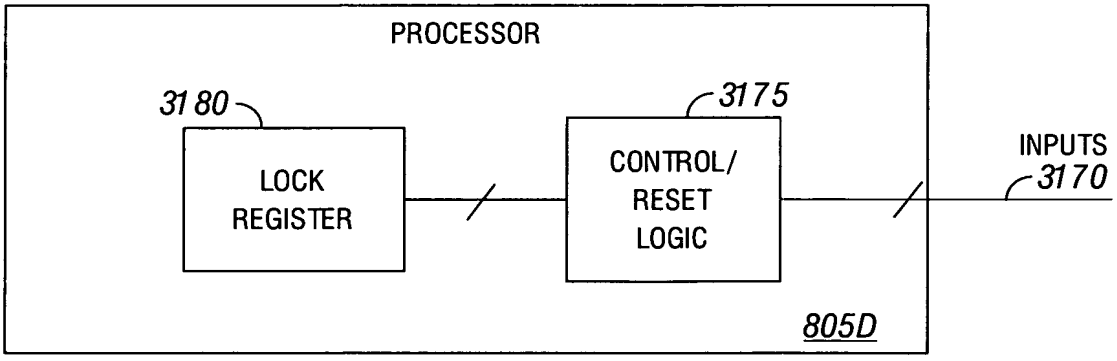

FIG. 20D

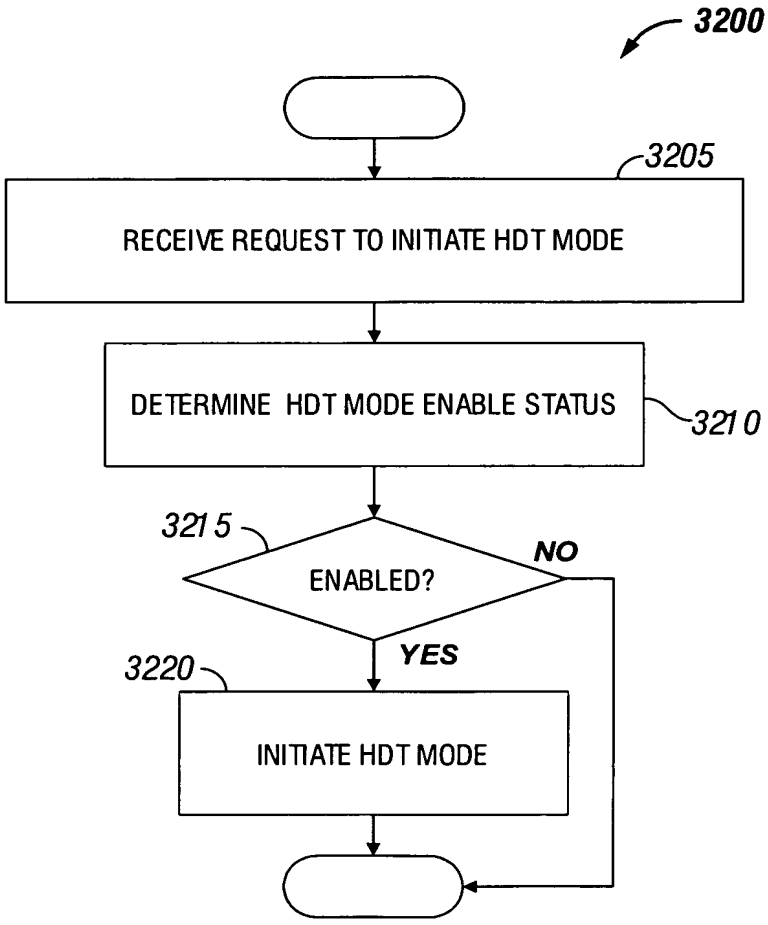
3200
3205
RECEIVE REQUEST TO INITIATE HDT MODE
DETERMINE HDT MODE ENABLE STATUS
3210
3215
ENABLED?
NO
YES
3220
INITIATE HDT MODE

FIG. 21

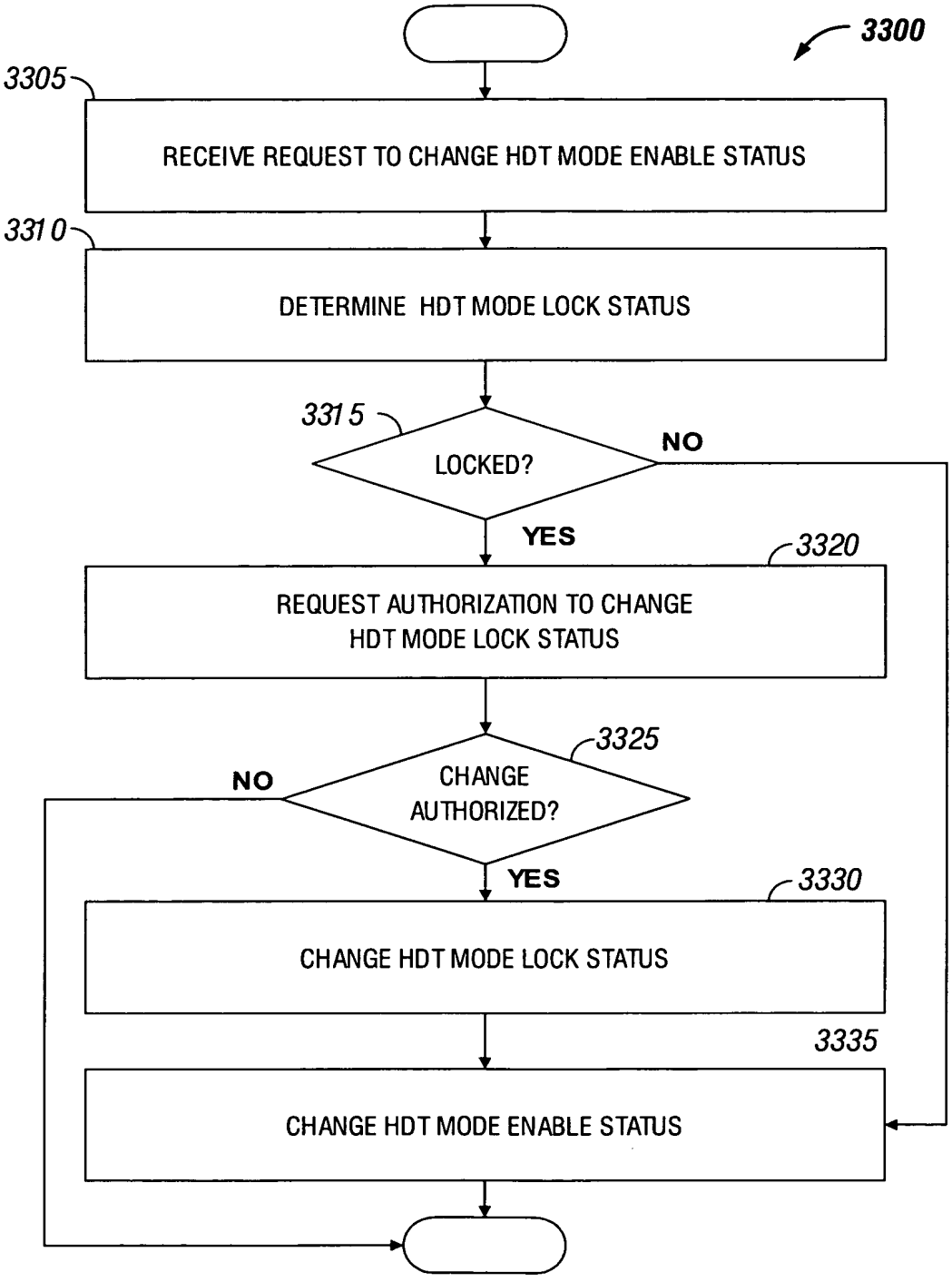
3300
3305
RECEIVE REQUEST TO CHANGE HDT MODE ENABLE STATUS
3310
DETERMINE HDT MODE LOCK STATUS
3315
LOCKED?
NO
YES
3320
REQUEST AUTHORIZATION TO CHANGE HDT MODE LOCK STATUS
3325
CHANGE AUTHORIZED?
NO
YES
3330
CHANGE HDT MODE LOCK STATUS
3335
CHANGE HDT MODE ENABLE STATUS

FIG. 22

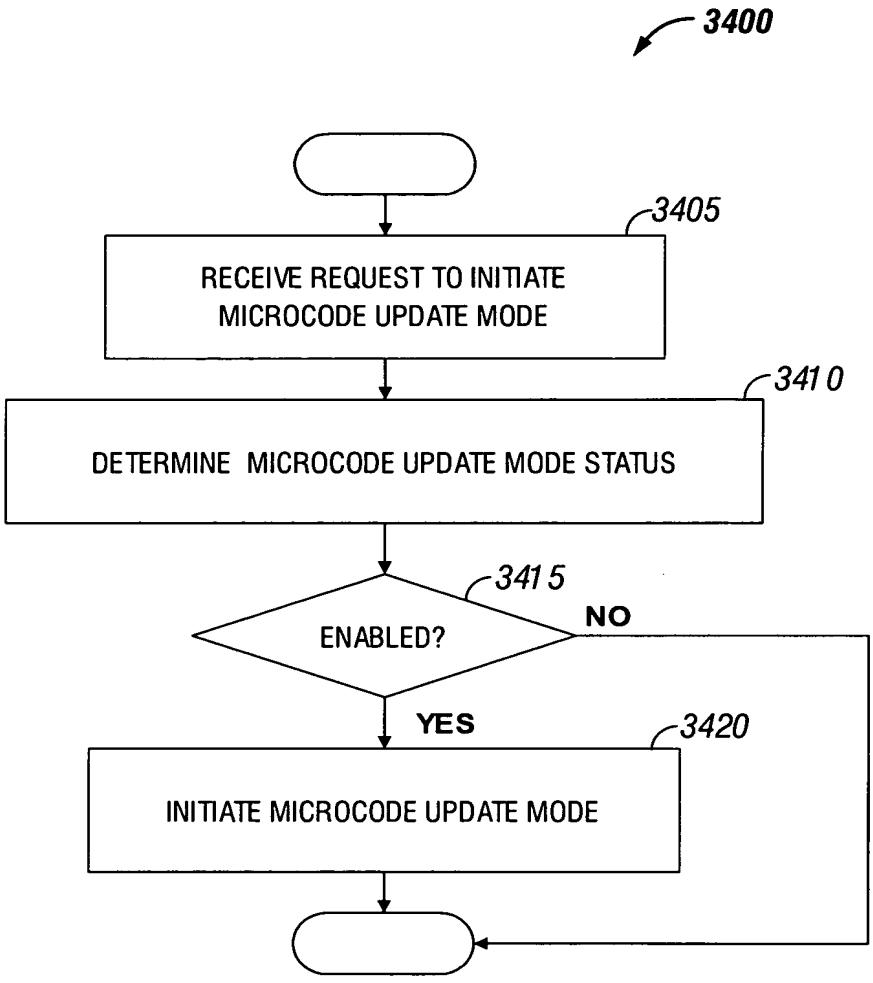
3400
3405
RECEIVE REQUEST TO INITIATE MICROCODE UPDATE MODE
3410
DETERMINE MICROCODE UPDATE MODE STATUS
3415
ENABLED?
NO
YES
3420
INITIATE MICROCODE UPDATE MODE

FIG. 23

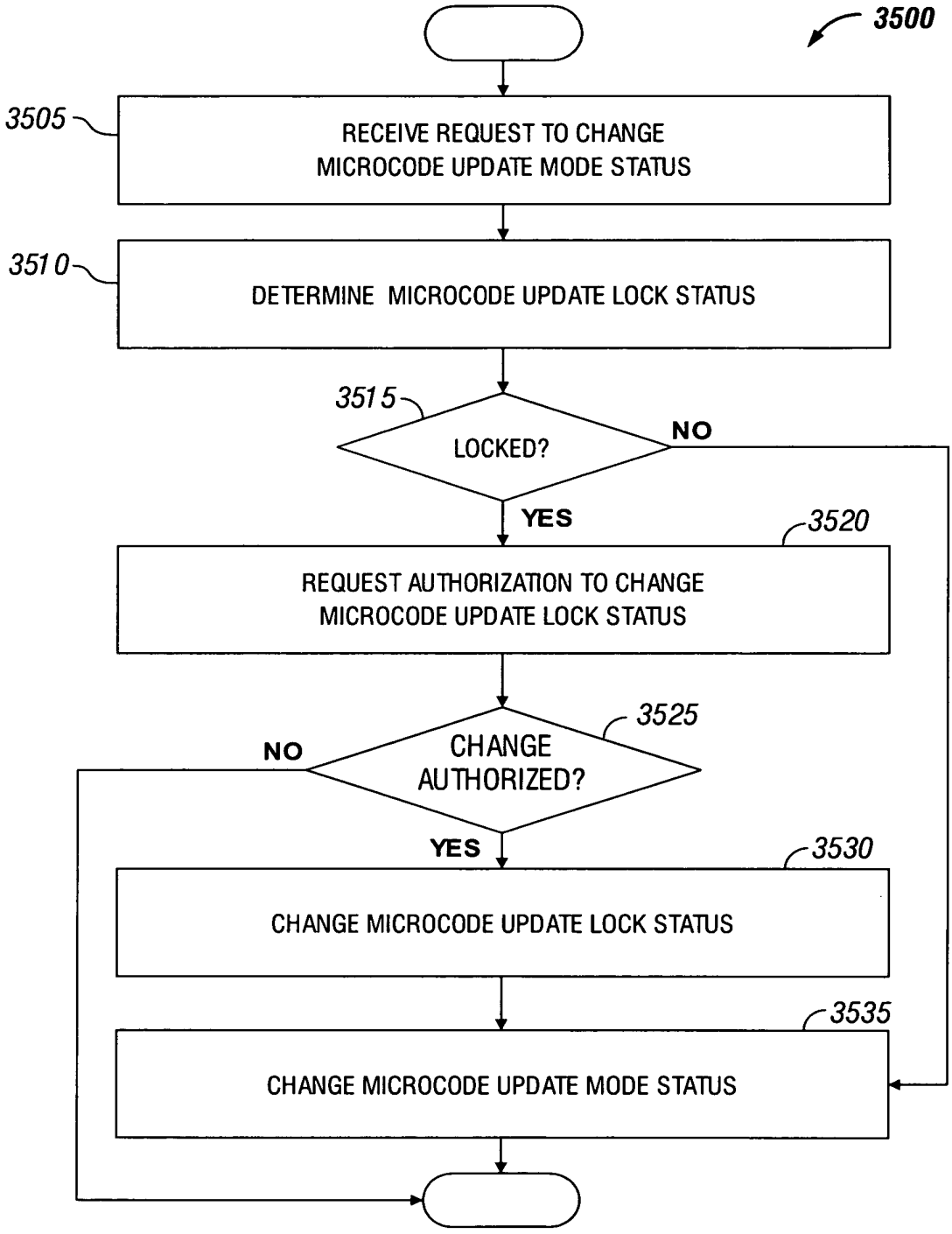
3500
3505
RECEIVE REQUEST TO CHANGE MICROCODE UPDATE MODE STATUS
3510
DETERMINE MICROCODE UPDATE LOCK STATUS
3515
LOCKED?
NO
YES
3520
REQUEST AUTHORIZATION TO CHANGE MICROCODE UPDATE LOCK STATUS
3525
CHANGE AUTHORIZED?
NO
YES
3530
CHANGE MICROCODE UPDATE LOCK STATUS
3535
CHANGE MICROCODE UPDATE MODE STATUS

FIG. 24

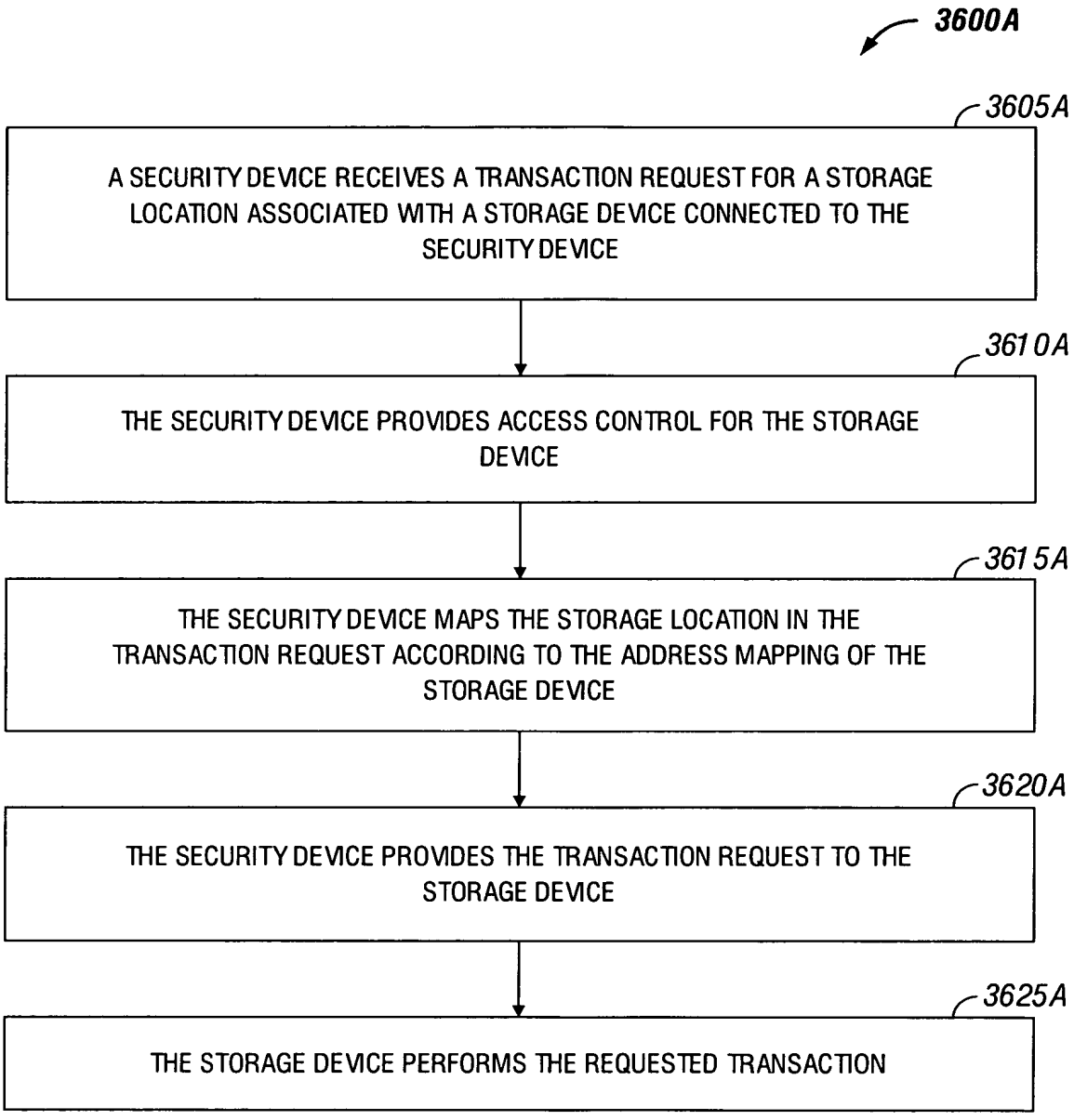
3600A
3605A
A SECURITY DEVICE RECEIVES A TRANSACTION REQUEST FOR A STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE
3610A
THE SECURITY DEVICE PROVIDES ACCESS CONTROL FOR THE STORAGE DEVICE
3615A
THE SECURITY DEVICE MAPS THE STORAGE LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE STORAGE DEVICE
3620A
THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE
3625A
THE STORAGE DEVICE PERFORMS THE REQUESTED TRANSACTION

FIG. 25A

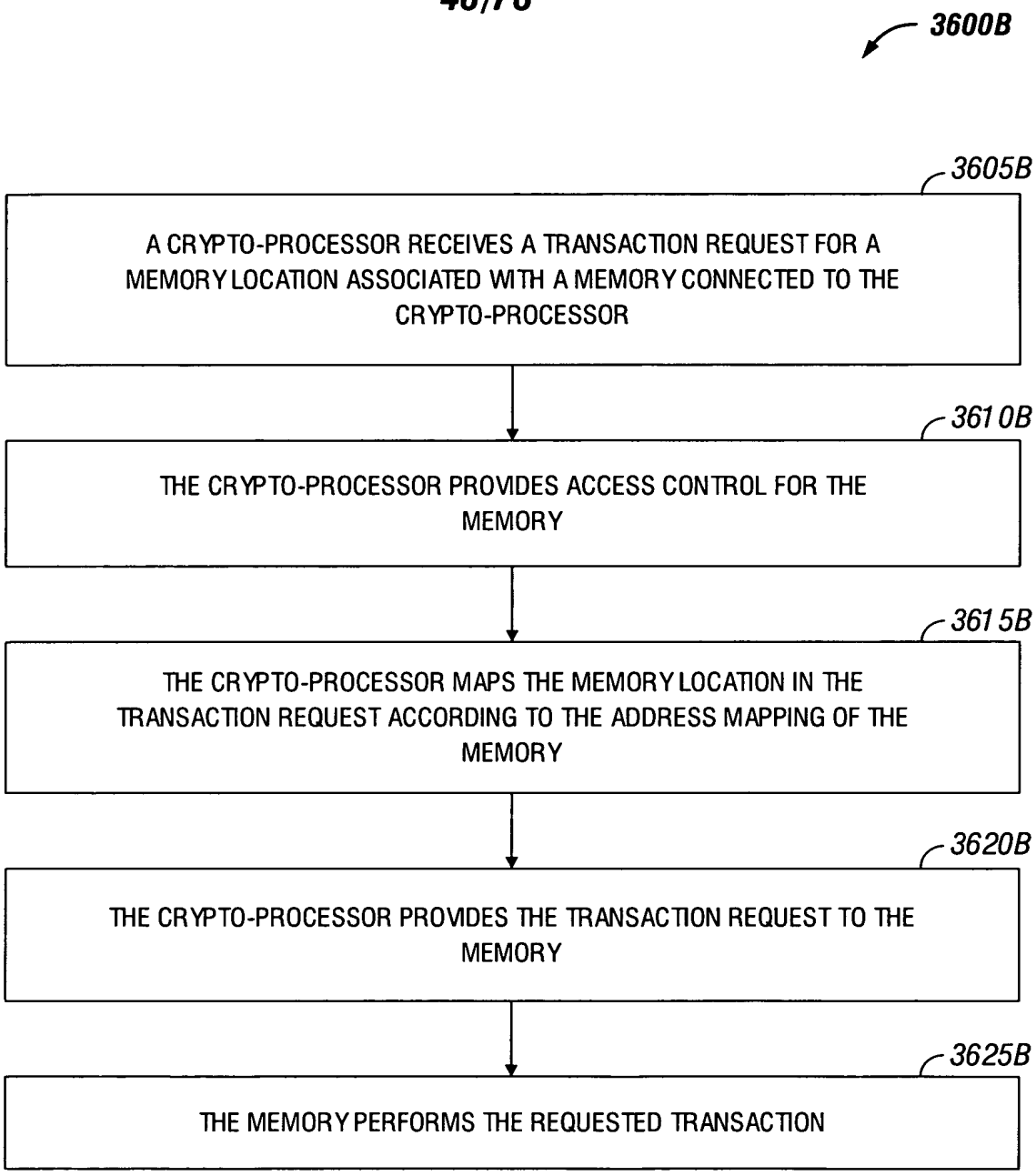
3600B
3605B
A CRYPTO-PROCESSOR RECEIVES A TRANSACTION REQUEST FOR A MEMORY LOCATION ASSOCIATED WITH A MEMORY CONNECTED TO THE CRYPTO-PROCESSOR
3610B
THE CRYPTO-PROCESSOR PROVIDES ACCESS CONTROL FOR THE MEMORY
3615B
THE CRYPTO-PROCESSOR MAPS THE MEMORY LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE MEMORY
3620B
THE CRYPTO-PROCESSOR PROVIDES THE TRANSACTION REQUEST TO THE MEMORY
3625B
THE MEMORY PERFORMS THE REQUESTED TRANSACTION

FIG. 25B

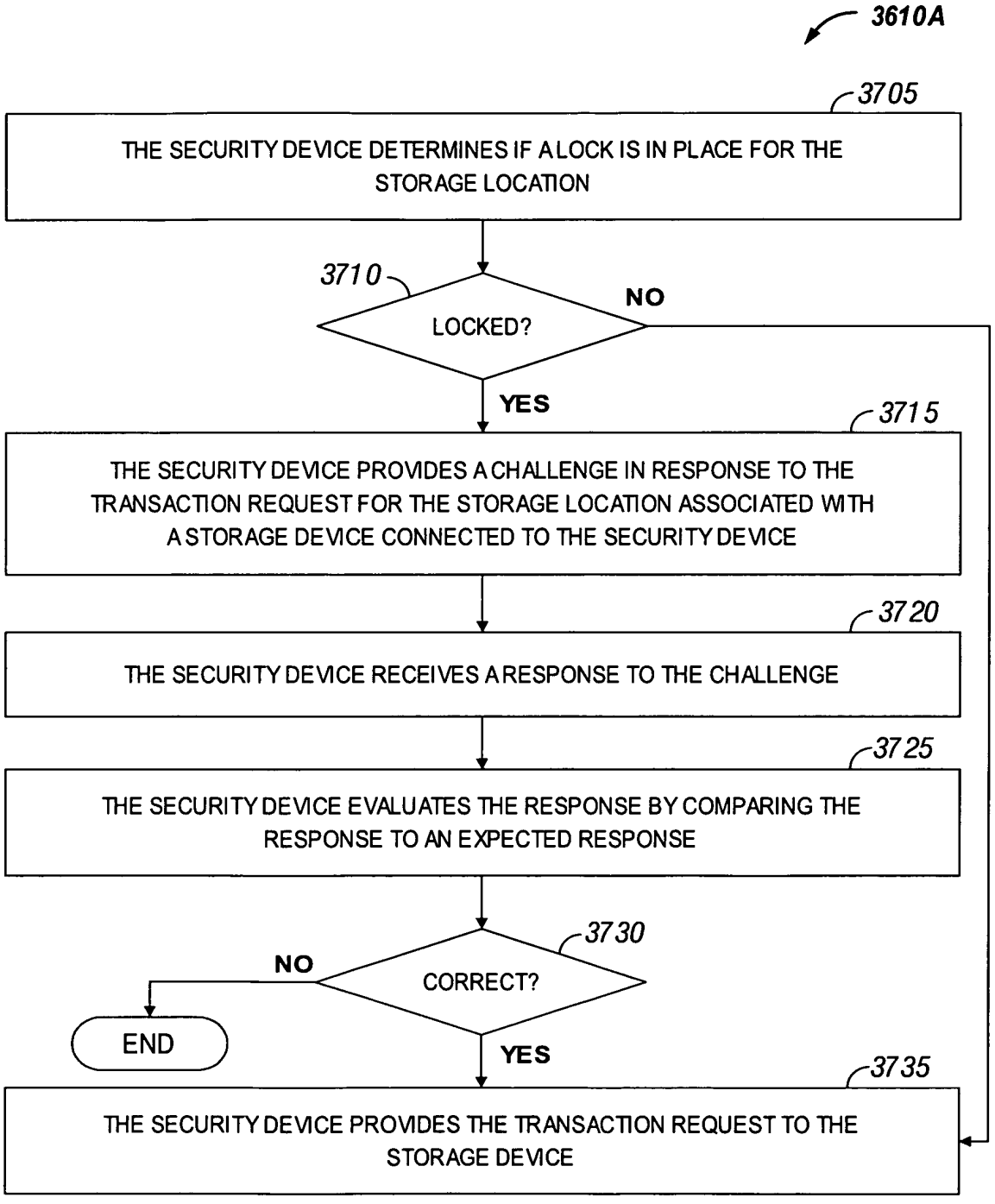
3610A
3705
THE SECURITY DEVICE DETERMINES IF A LOCK IS IN PLACE FOR THE STORAGE LOCATION
3710
LOCKED?
NO
YES
3715
THE SECURITY DEVICE PROVIDES A CHALLENGE IN RESPONSE TO THE TRANSACTION REQUEST FOR THE STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE
3720
THE SECURITY DEVICE RECEIVES A RESPONSE TO THE CHALLENGE
3725
THE SECURITY DEVICE EVALUATES THE RESPONSE BY COMPARING THE RESPONSE TO AN EXPECTED RESPONSE
3730
CORRECT?
NO
END
YES
3735
THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE

FIG. 26

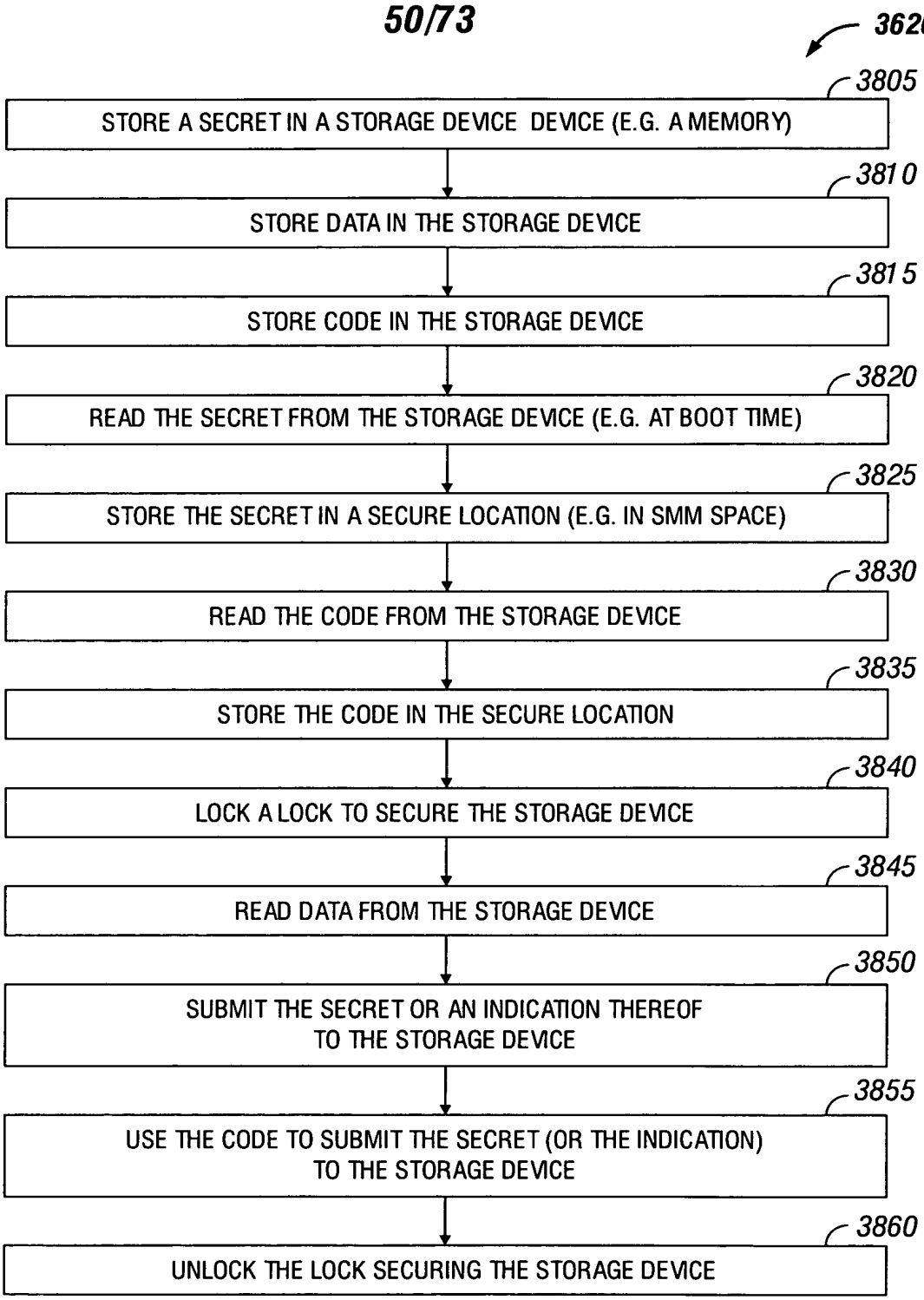
3620
3805
STORE A SECRET IN A STORAGE DEVICE DEVICE (E.G. A MEMORY)
3810
STORE DATA IN THE STORAGE DEVICE
3815
STORE CODE IN THE STORAGE DEVICE
3820
READ THE SECRET FROM THE STORAGE DEVICE (E.G. AT BOOT TIME)
3825
STORE THE SECRET IN A SECURE LOCATION (E.G. IN SMM SPACE)
3830
READ THE CODE FROM THE STORAGE DEVICE
3835
STORE THE CODE IN THE SECURE LOCATION
3840
LOCK A LOCK TO SECURE THE STORAGE DEVICE
3845
READ DATA FROM THE STORAGE DEVICE
3850
SUBMIT THE SECRET OR AN INDICATION THEREOF TO THE STORAGE DEVICE
3855
USE THE CODE TO SUBMIT THE SECRET (OR THE INDICATION) TO THE STORAGE DEVICE
3860
UNLOCK THE LOCK SECURING THE STORAGE DEVICE

FIG. 27

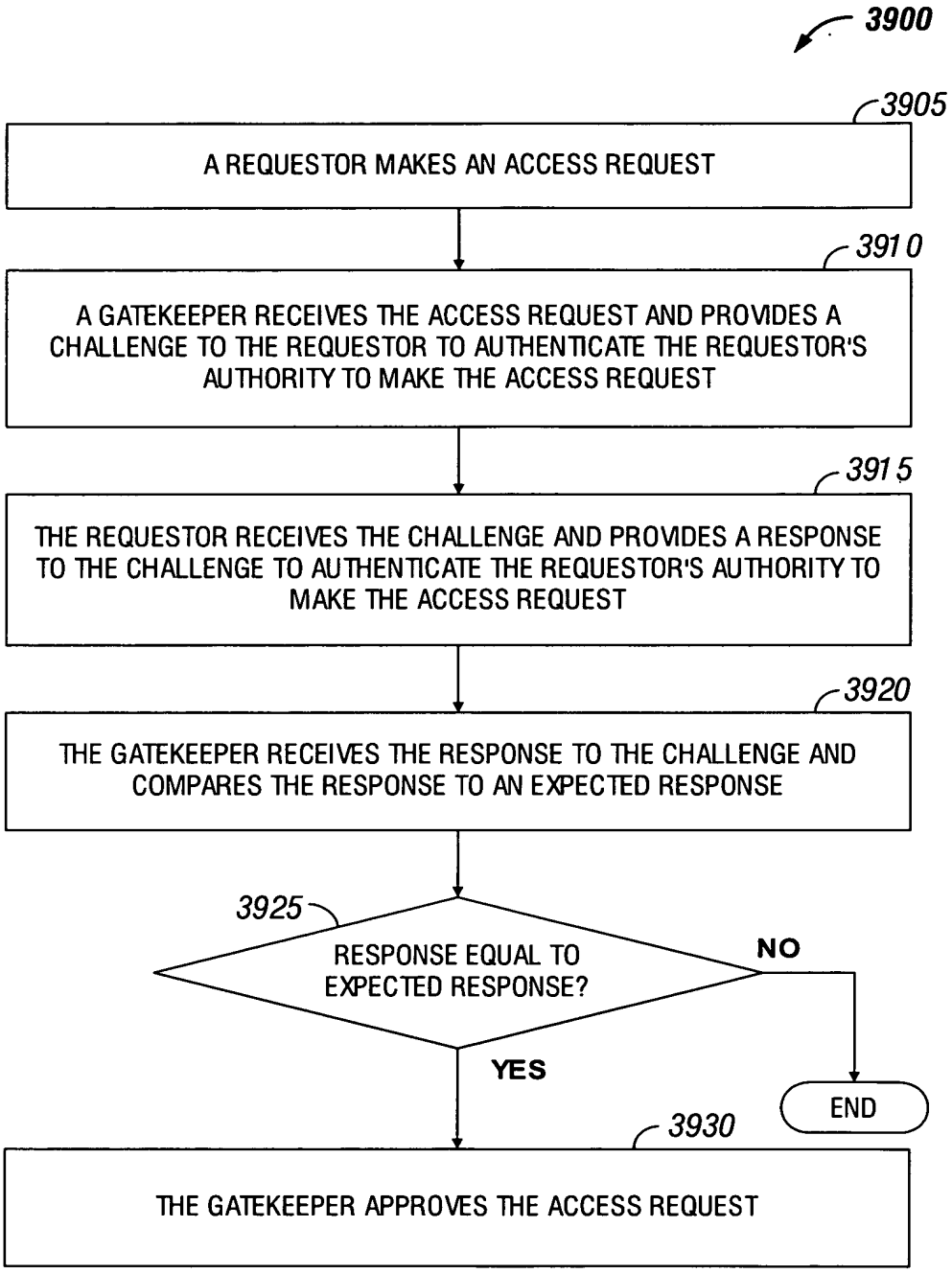

FIG. 28
(Prior Art)

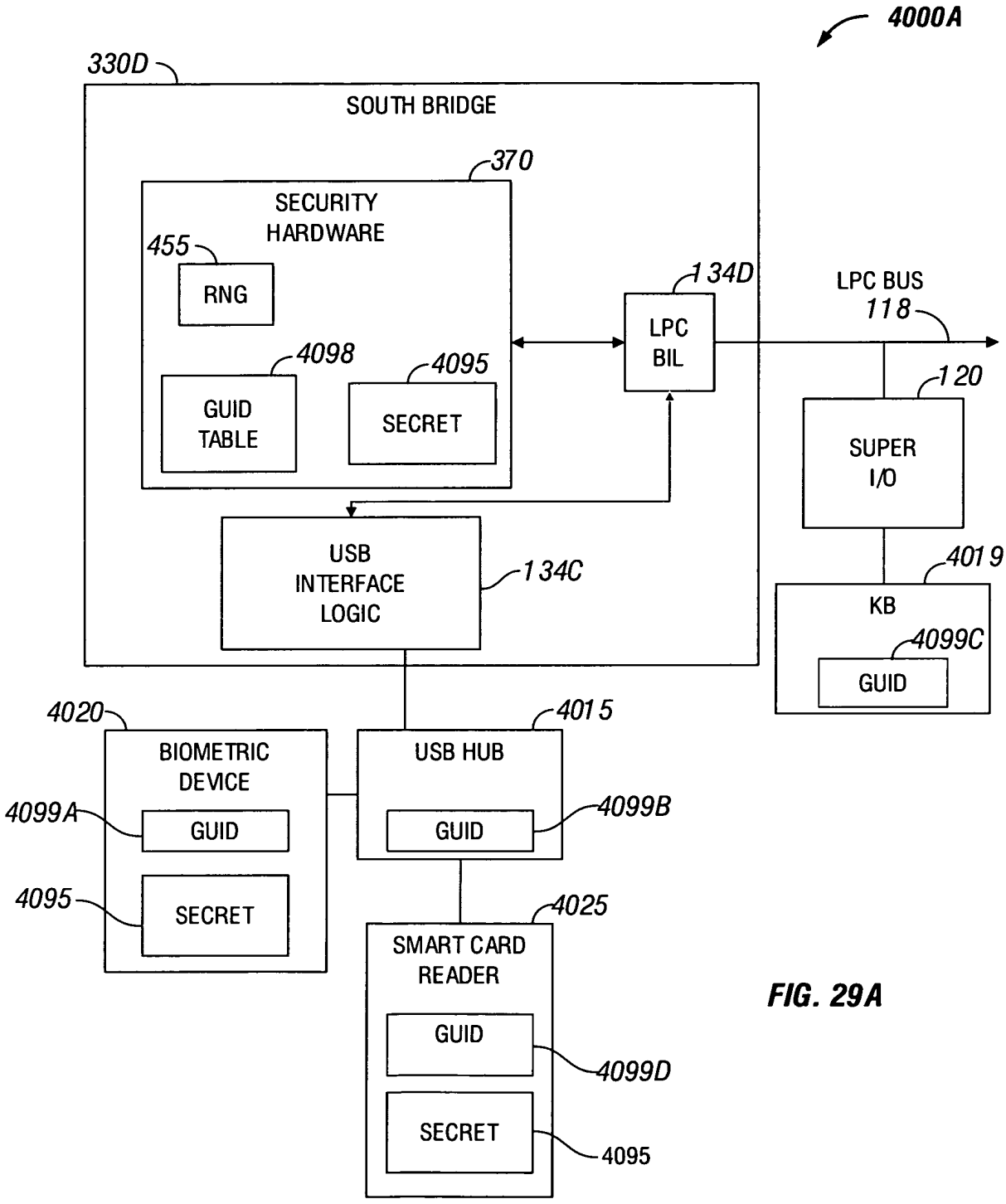
4000A
330D
SOUTH BRIDGE
370
SECURITY HARDWARE
455
RNG
4098
GUID TABLE
4095
SECRET
134D
LPC BIL
LPC BUS
118
120
SUPER I/O
4019
KB
4099C
GUID
USB INTERFACE LOGIC
134C
4020
BIOMETRIC DEVICE
4099A
GUID
4095
SECRET
4015
USB HUB
GUID
4099B
4025
SMART CARD READER
GUID
4099D
SECRET
4095

FIG. 29A

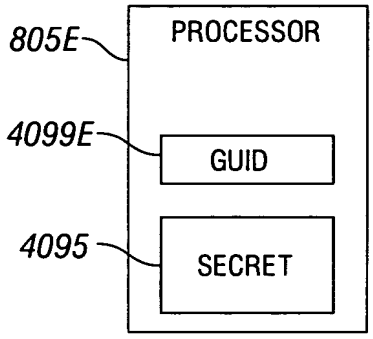

FIG. 29B

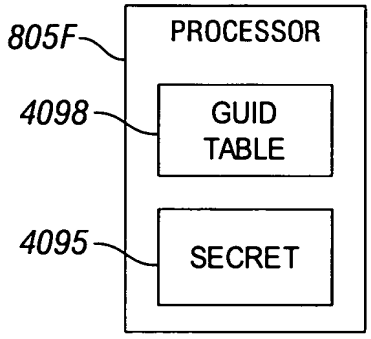

FIG. 29C

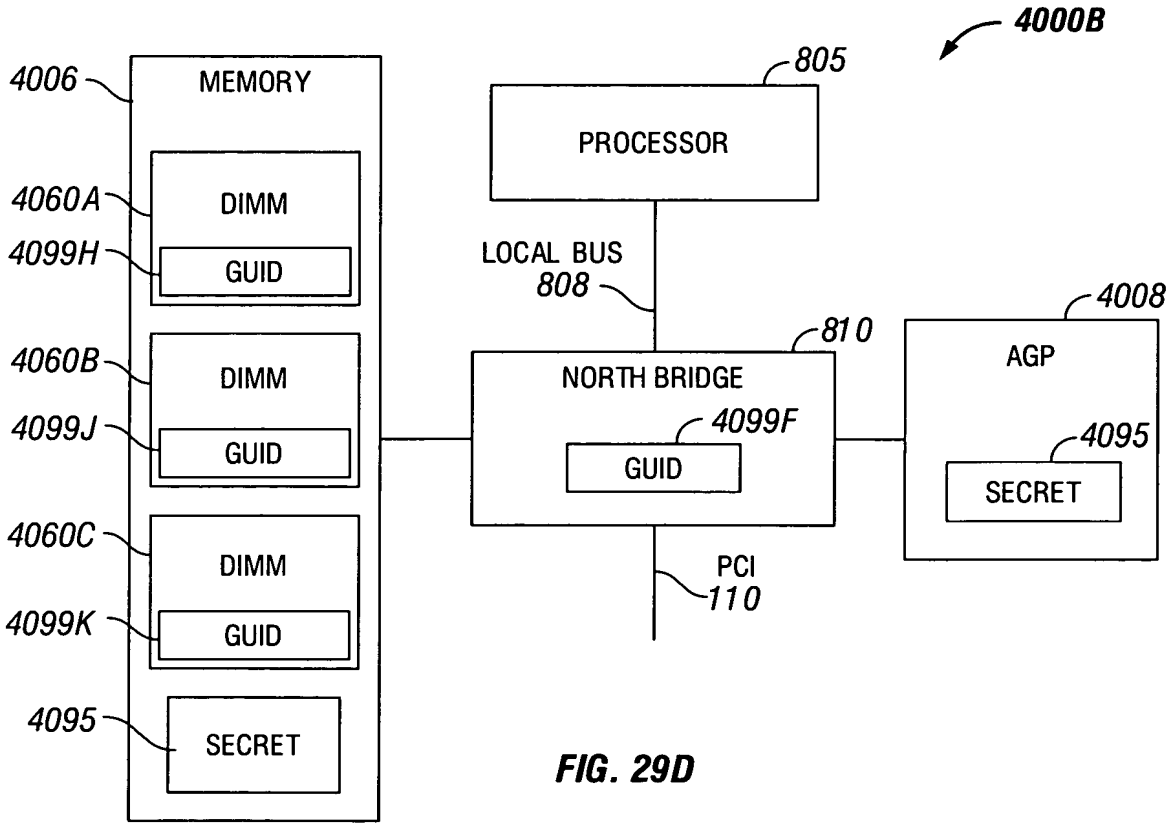

FIG. 29D

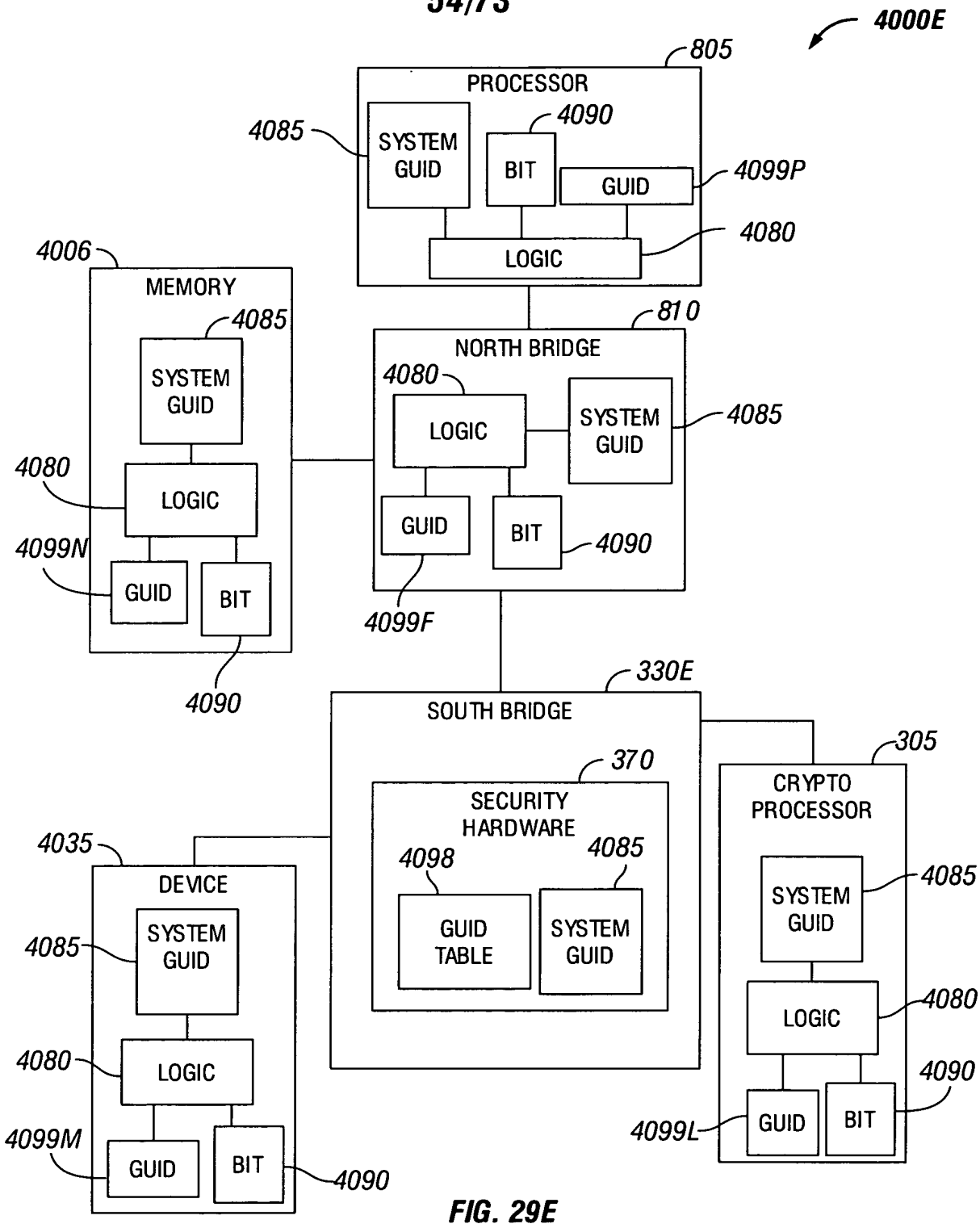
4000E
805
PROCESSOR
4085
SYSTEM GUID
4090
BIT
GUID
4099P
LOGIC
4080
4006
MEMORY
4085
SYSTEM GUID
4080
LOGIC
4099N
GUID
BIT
4090
810
NORTH BRIDGE
4080
LOGIC
SYSTEM GUID
4085
GUID
BIT
4090
4099F
330E
SOUTH BRIDGE
370
SECURITY HARDWARE
4098
4085
GUID TABLE
SYSTEM GUID
305
CRYPTO PROCESSOR
4085
SYSTEM GUID
LOGIC
4080
4090
4099L
GUID
BIT
4035
DEVICE
4085
SYSTEM GUID
4080
LOGIC
4099M
GUID
BIT
4090

FIG. 29E

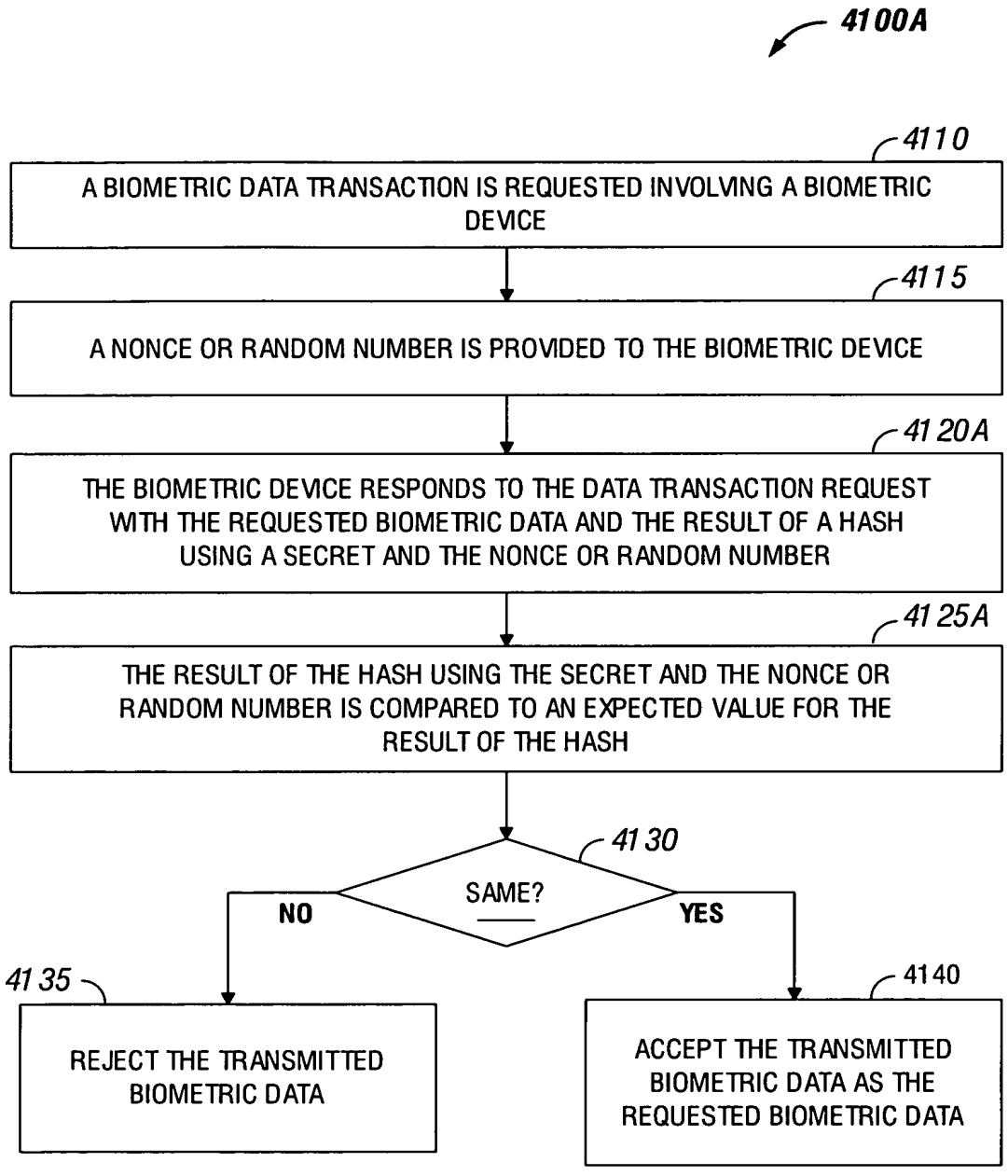
4100A
4110
A BIOMETRIC DATA TRANSACTION IS REQUESTED INVOLVING A BIOMETRIC DEVICE
4115
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE BIOMETRIC DEVICE
4120A
THE BIOMETRIC DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED BIOMETRIC DATA AND THE RESULT OF A HASH USING A SECRET AND THE NONCE OR RANDOM NUMBER
4125A
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH
4130
SAME?
NO
YES
4135
REJECT THE TRANSMITTED BIOMETRIC DATA
4140
ACCEPT THE TRANSMITTED BIOMETRIC DATA AS THE REQUESTED BIOMETRIC DATA

FIG. 30A

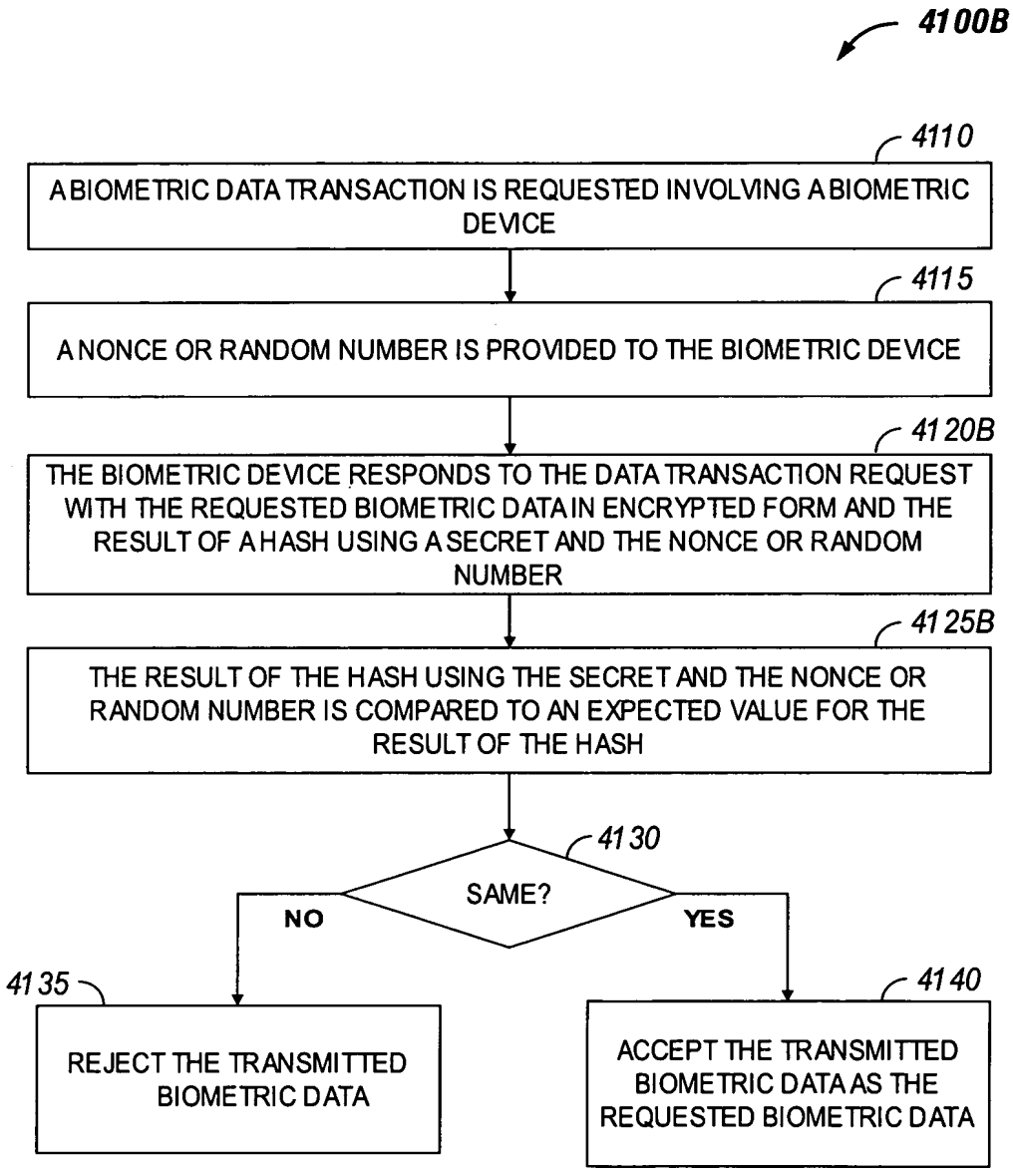
4100B
4110
A BIOMETRIC DATA TRANSACTION IS REQUESTED INVOLVING A BIOMETRIC DEVICE
4115
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE BIOMETRIC DEVICE
4120B
THE BIOMETRIC DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED BIOMETRIC DATA IN ENCRYPTED FORM AND THE RESULT OF A HASH USING A SECRET AND THE NONCE OR RANDOM NUMBER
4125B
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH
4130
SAME?
NO
YES
4135
REJECT THE TRANSMITTED BIOMETRIC DATA
4140
ACCEPT THE TRANSMITTED BIOMETRIC DATA AS THE REQUESTED BIOMETRIC DATA

FIG. 30B

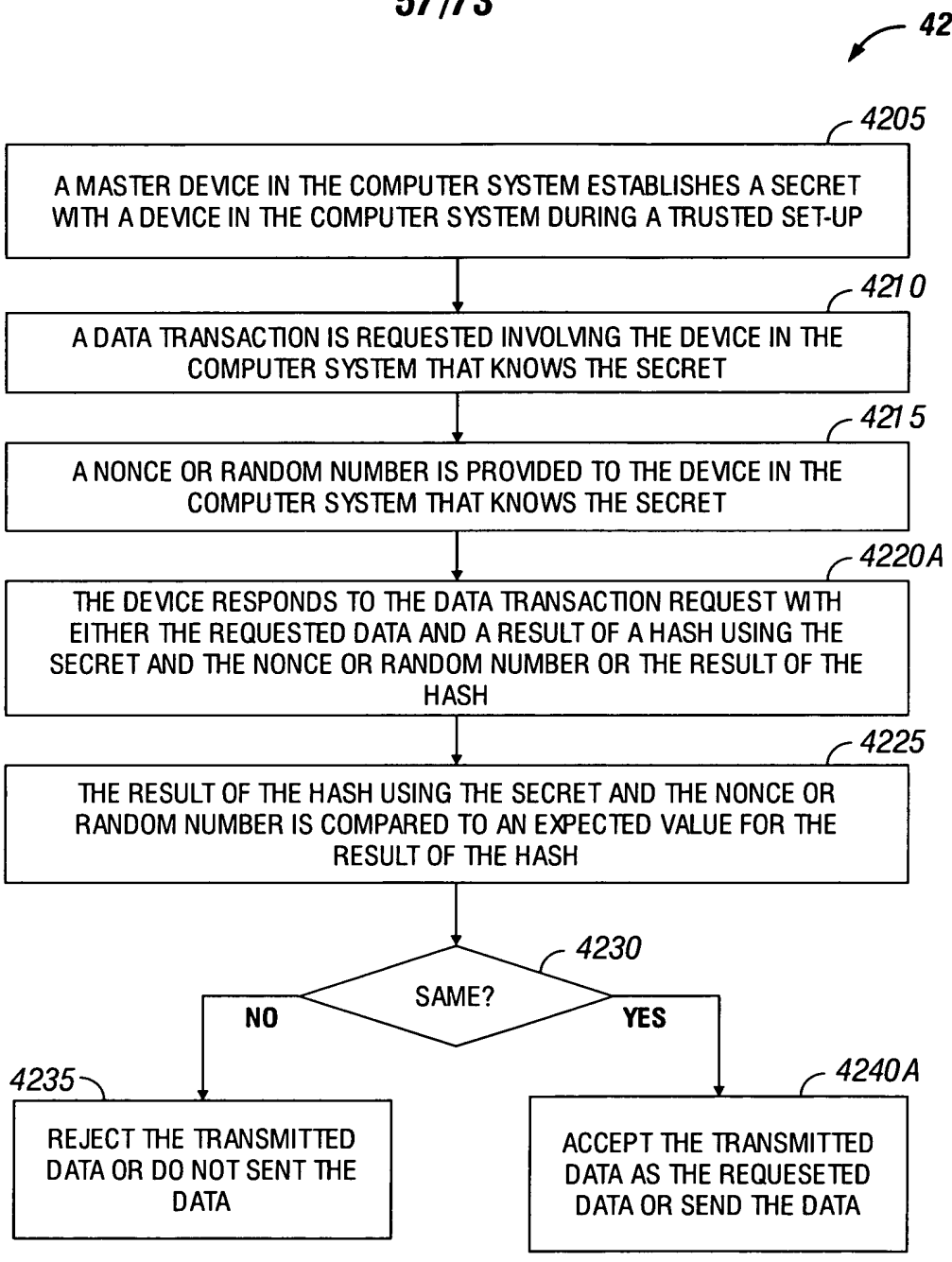
4200A
4205
A MASTER DEVICE IN THE COMPUTER SYSTEM ESTABLISHES A SECRET WITH A DEVICE IN THE COMPUTER SYSTEM DURING A TRUSTED SET-UP
4210
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET
4215
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET
4220A
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH EITHER THE REQUESTED DATA AND A RESULT OF A HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER OR THE RESULT OF THE HASH
4225
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH
4230
SAME?
NO
YES
4235
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA
4240A
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR SEND THE DATA

FIG. 31A

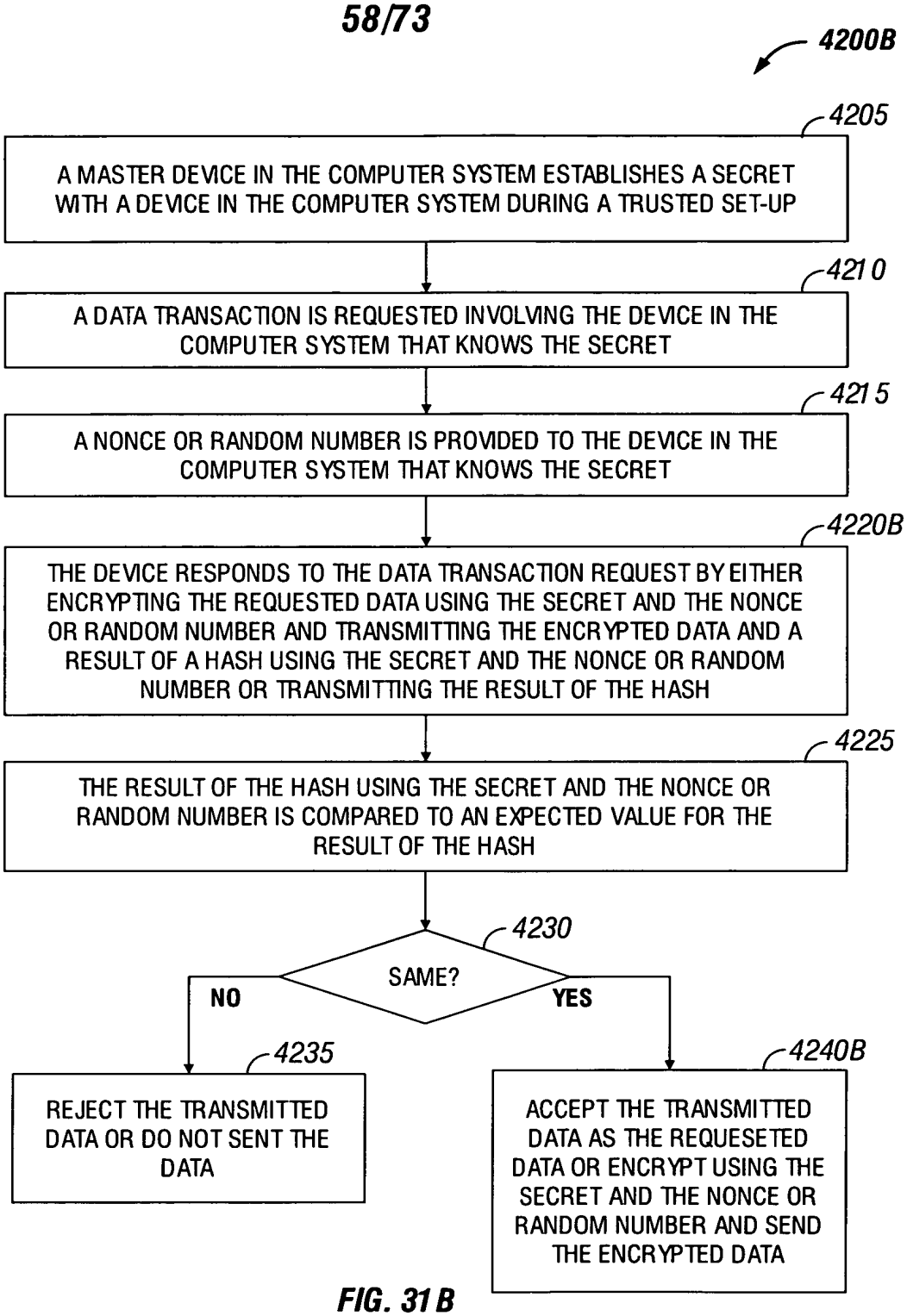
4200B
4205
A MASTER DEVICE IN THE COMPUTER SYSTEM ESTABLISHES A SECRET WITH A DEVICE IN THE COMPUTER SYSTEM DURING A TRUSTED SET-UP
4210
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET
4215
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET
4220B
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY EITHER ENCRYPTING THE REQUESTED DATA USING THE SECRET AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH
4225
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH
4230
SAME?
NO
YES
4235
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA
4240B
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR ENCRYPT USING THE SECRET AND THE NONCE OR RANDOM NUMBER AND SEND THE ENCRYPTED DATA

FIG. 31B

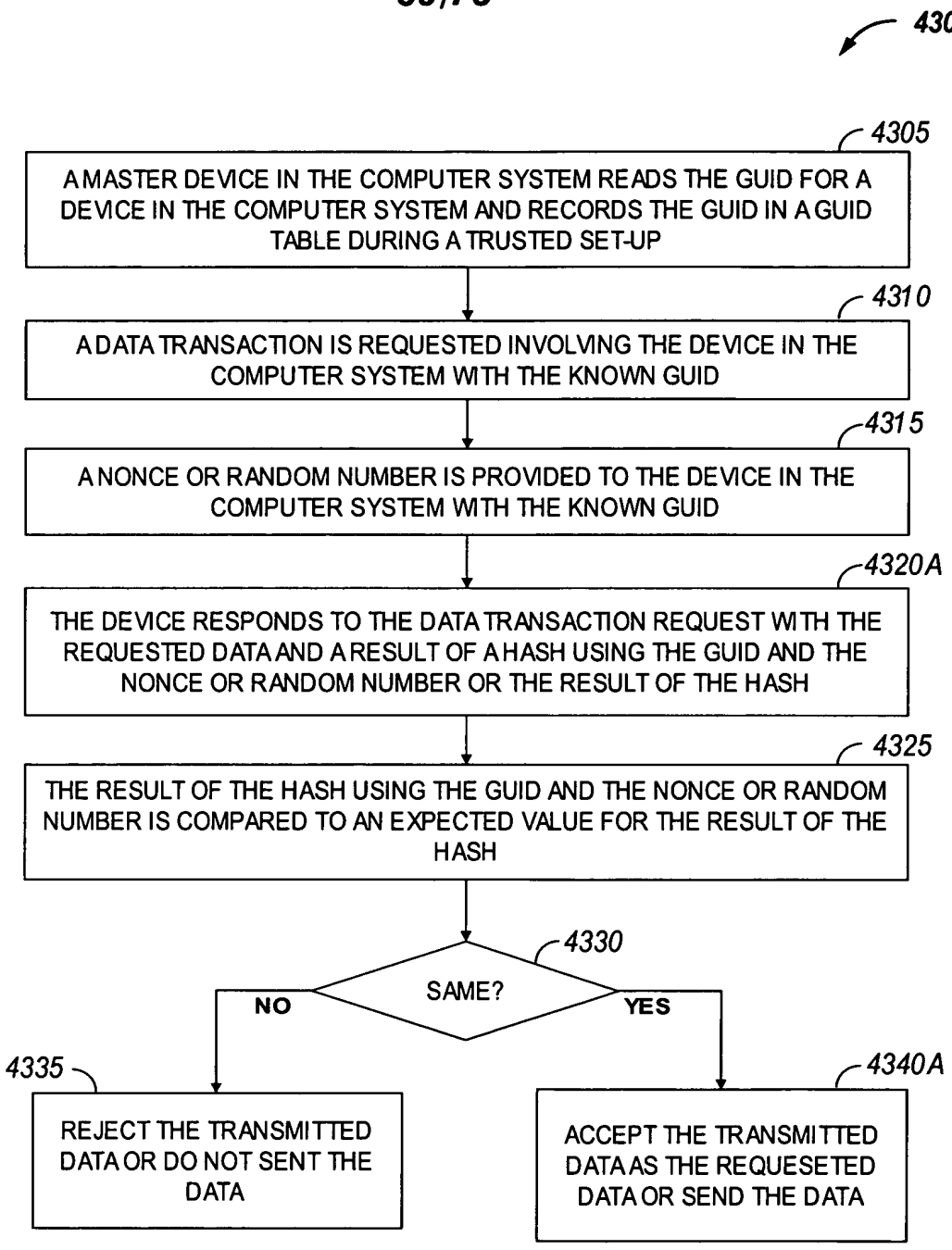
4300A
4305
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP
4310
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID
4315
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID
4320A
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED DATA AND A RESULT OF A HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER OR THE RESULT OF THE HASH
4325
THE RESULT OF THE HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH
4330
SAME?
NO
YES
4335
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA
4340A
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR SEND THE DATA

FIG. 32A

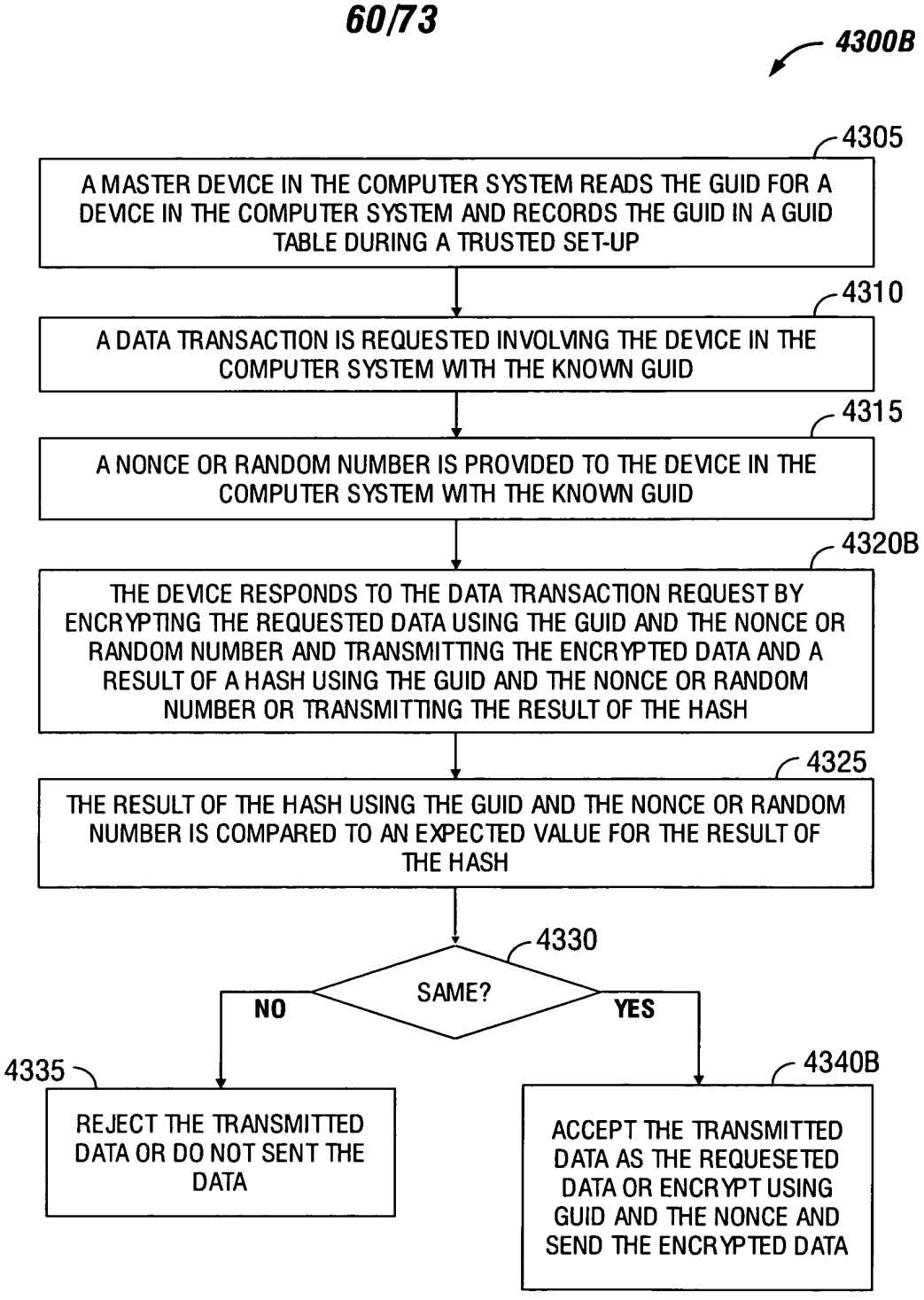
4300B
4305
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP
4310
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID
4315
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID
4320B
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY ENCRYPTING THE REQUESTED DATA USING THE GUID AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH
4325
THE RESULT OF THE HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH
4330
SAME?
NO
YES
4335
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA
4340B
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR ENCRYPT USING GUID AND THE NONCE AND SEND THE ENCRYPTED DATA

FIG. 32B

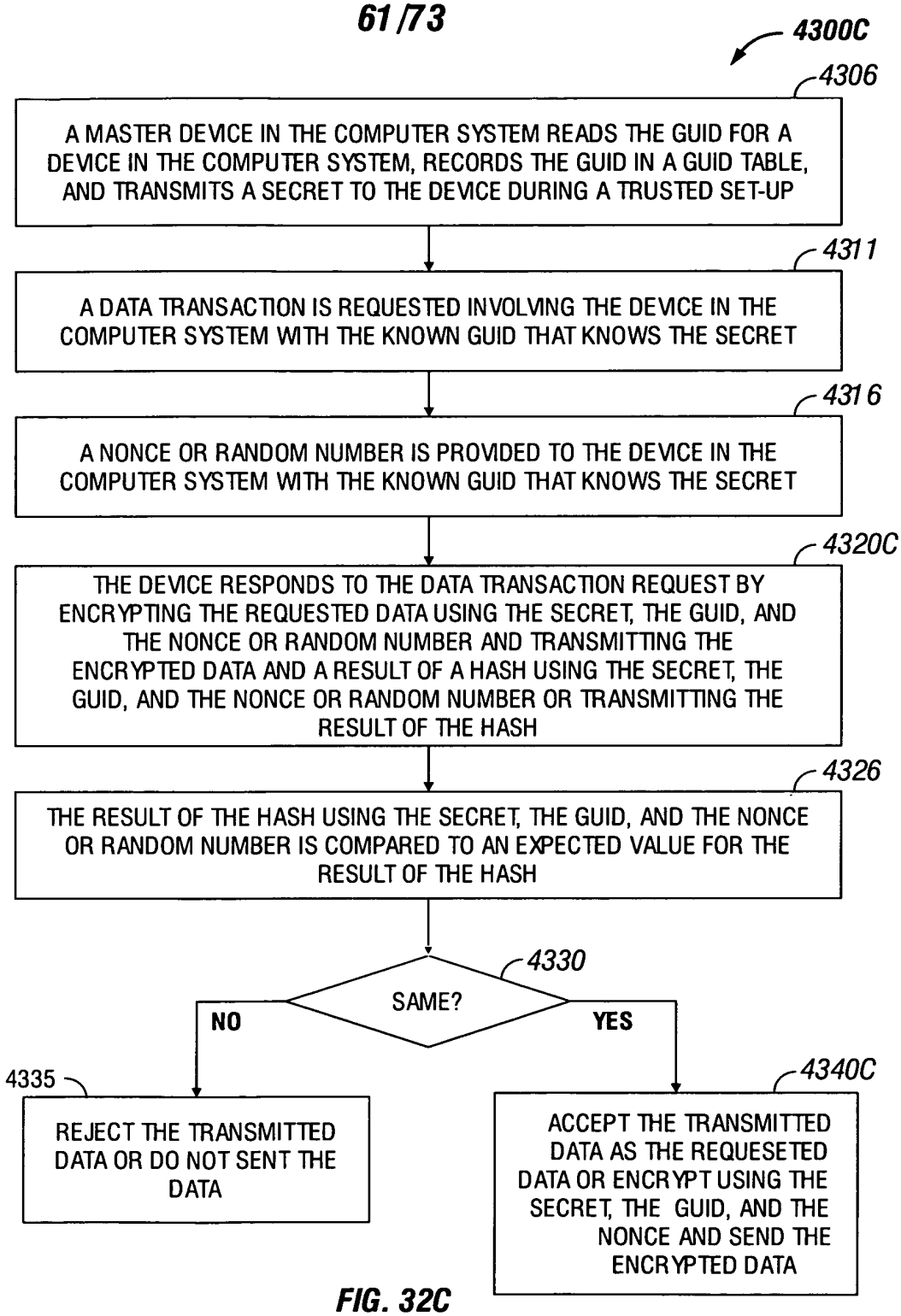
4300C
4306
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM, RECORDS THE GUID IN A GUID TABLE, AND TRANSMITS A SECRET TO THE DEVICE DURING A TRUSTED SET-UP
4311
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET
4316
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET
4320C
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY ENCRYPTING THE REQUESTED DATA USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH
4326
THE RESULT OF THE HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH
4330
SAME?
NO
YES
4335
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA
4340C
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR ENCRYPT USING THE SECRET, THE GUID, AND THE NONCE AND SEND THE ENCRYPTED DATA

FIG. 32C

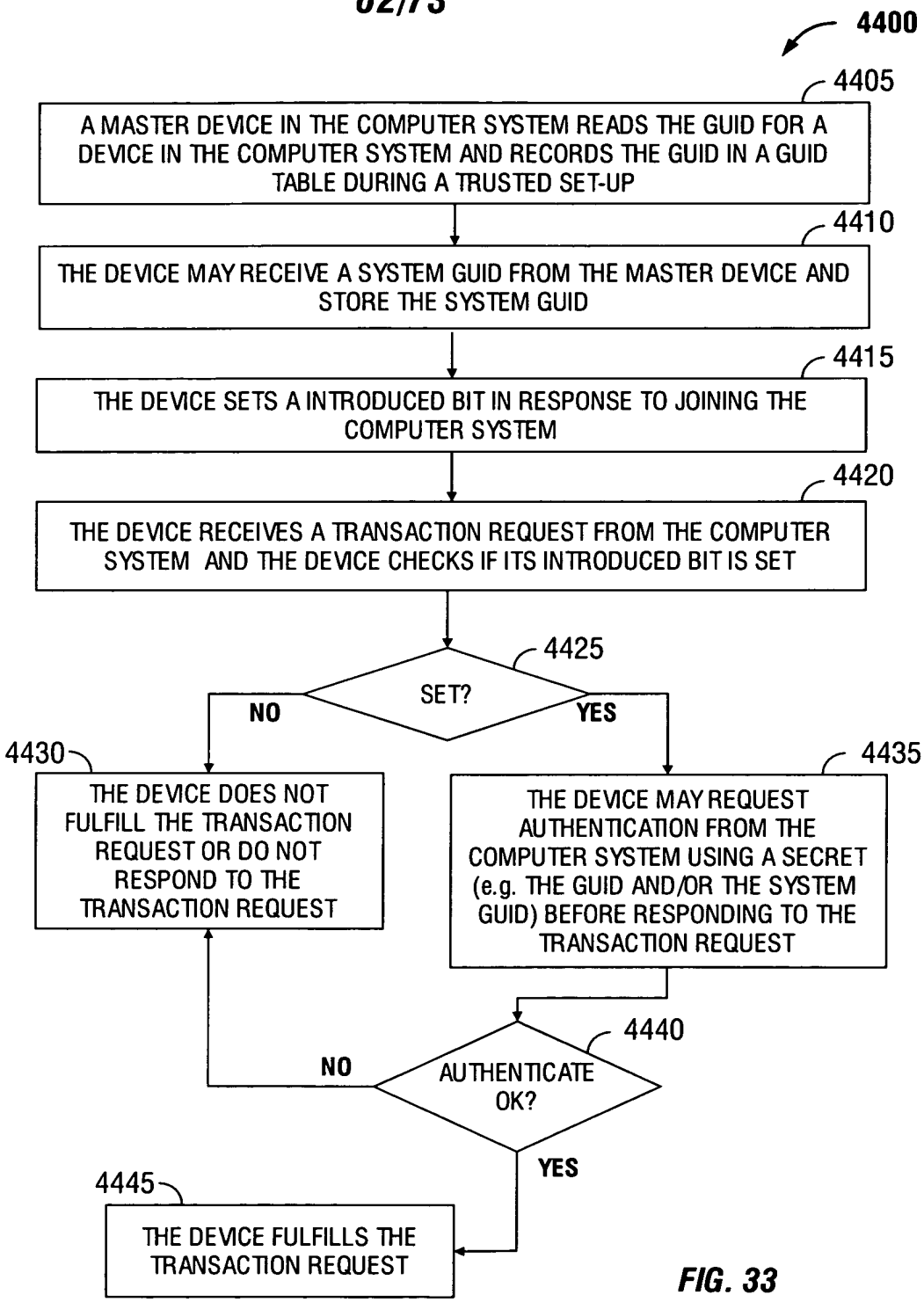
4400
4405
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP
4410
THE DEVICE MAY RECEIVE A SYSTEM GUID FROM THE MASTER DEVICE AND STORE THE SYSTEM GUID
4415
THE DEVICE SETS A INTRODUCED BIT IN RESPONSE TO JOINING THE COMPUTER SYSTEM
4420
THE DEVICE RECEIVES A TRANSACTION REQUEST FROM THE COMPUTER SYSTEM AND THE DEVICE CHECKS IF ITS INTRODUCED BIT IS SET
4425
SET?
NO
YES
4430
THE DEVICE DOES NOT FULFILL THE TRANSACTION REQUEST OR DO NOT RESPOND TO THE TRANSACTION REQUEST
4435
THE DEVICE MAY REQUEST AUTHENTICATION FROM THE COMPUTER SYSTEM USING A SECRET (e.g. THE GUID AND/OR THE SYSTEM GUID) BEFORE RESPONDING TO THE TRANSACTION REQUEST
4440
AUTHENTICATE OK?
NO
YES
4445
THE DEVICE FULFILLS THE TRANSACTION REQUEST

FIG. 33

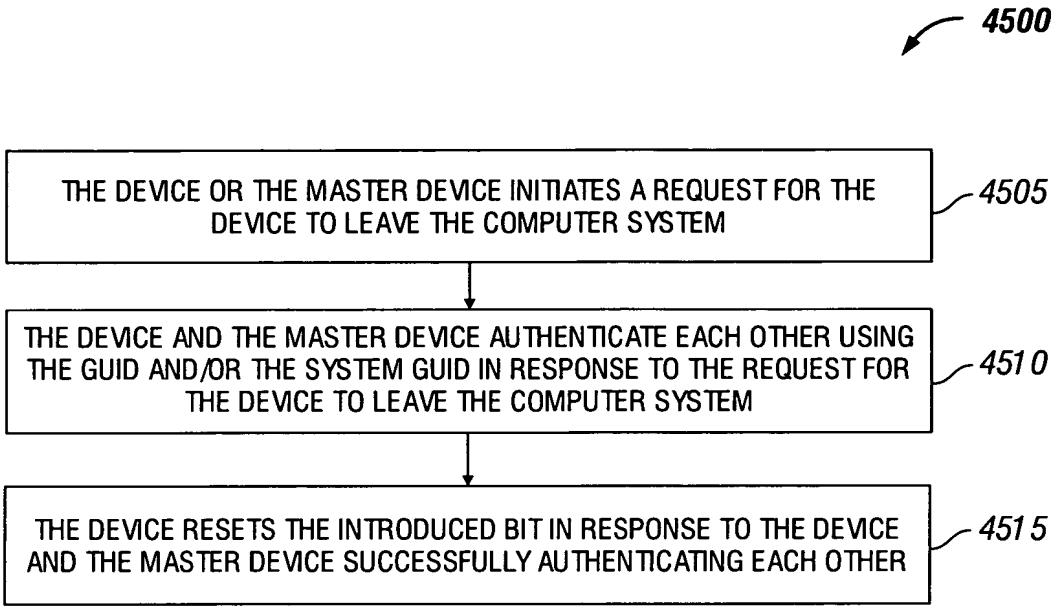
4500
THE DEVICE OR THE MASTER DEVICE INITIATES A REQUEST FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM
4505
THE DEVICE AND THE MASTER DEVICE AUTHENTICATE EACH OTHER USING THE GUID AND/OR THE SYSTEM GUID IN RESPONSE TO THE REQUEST FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM
4510
THE DEVICE RESETS THE INTRODUCED BIT IN RESPONSE TO THE DEVICE AND THE MASTER DEVICE SUCCESSFULLY AUTHENTICATING EACH OTHER
4515

FIG. 34

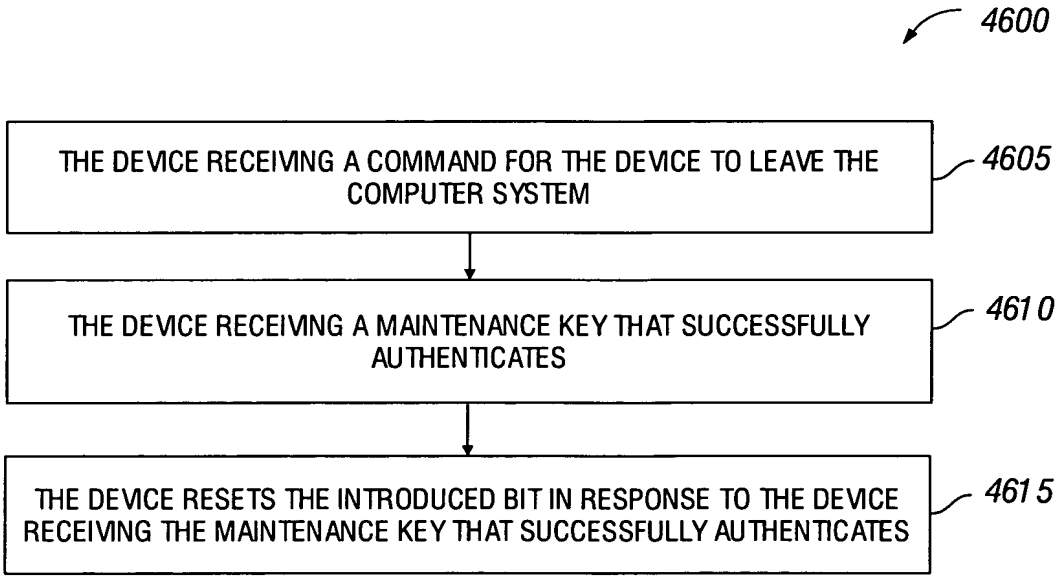
4600
THE DEVICE RECEIVING A COMMAND FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM
4605
THE DEVICE RECEIVING A MAINTENANCE KEY THAT SUCCESSFULLY AUTHENTICATES
4610
THE DEVICE RESETS THE INTRODUCED BIT IN RESPONSE TO THE DEVICE RECEIVING THE MAINTENANCE KEY THAT SUCCESSFULLY AUTHENTICATES
4615

FIG. 35

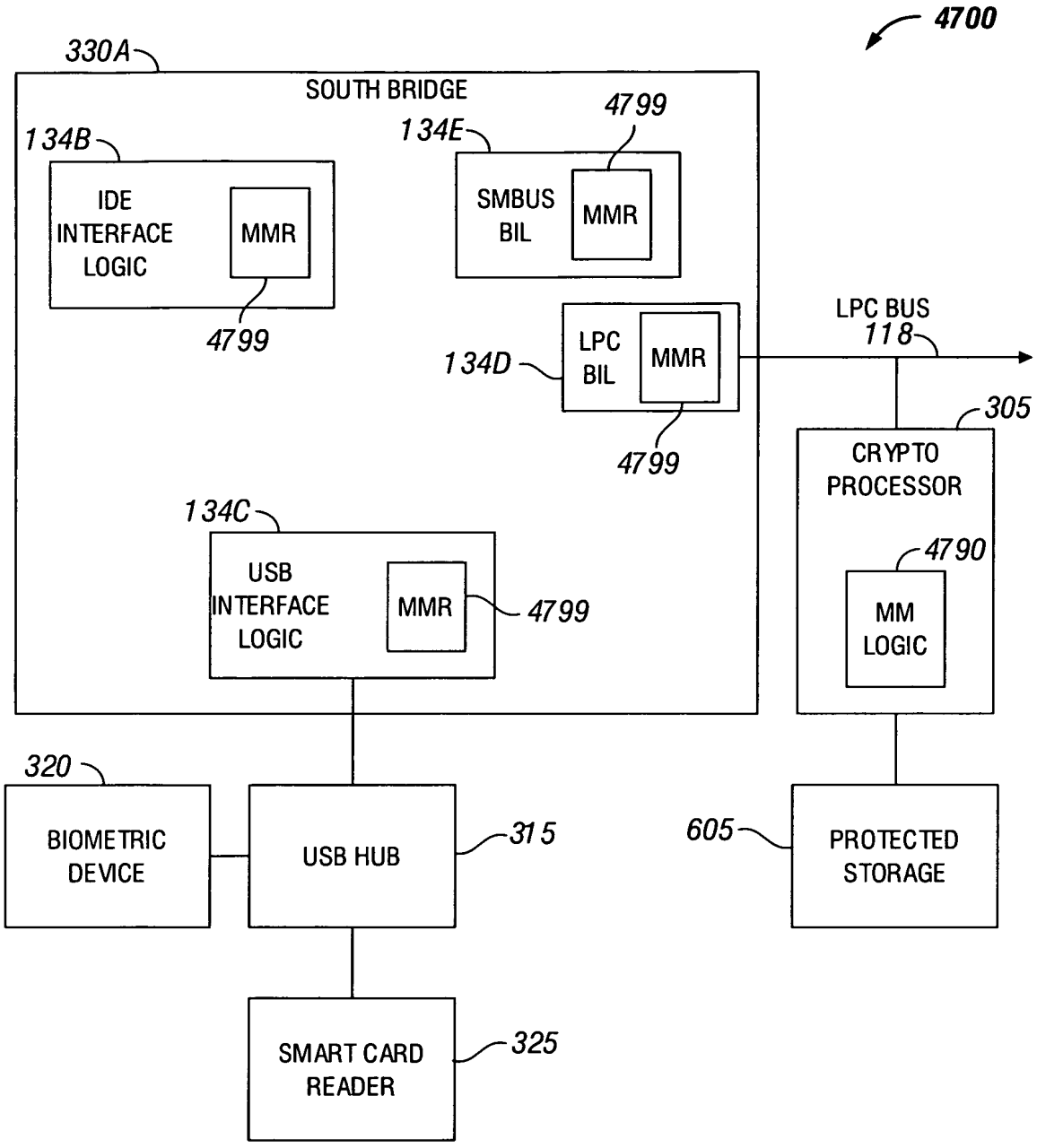
4700
330A
SOUTH BRIDGE
4799
134E
134B
IDE
INTERFACE
LOGIC
MMR
4799
SMBUS
BIL
MMR
LPC BUS
118
LPC
BIL
MMR
134D
4799
305
CRYPTO
PROCESSOR
4790
MM
LOGIC
134C
USB
INTERFACE
LOGIC
MMR
4799
320
BIOMETRIC
DEVICE
USB HUB
315
605
PROTECTED
STORAGE
SMART CARD
READER
325

FIG. 36

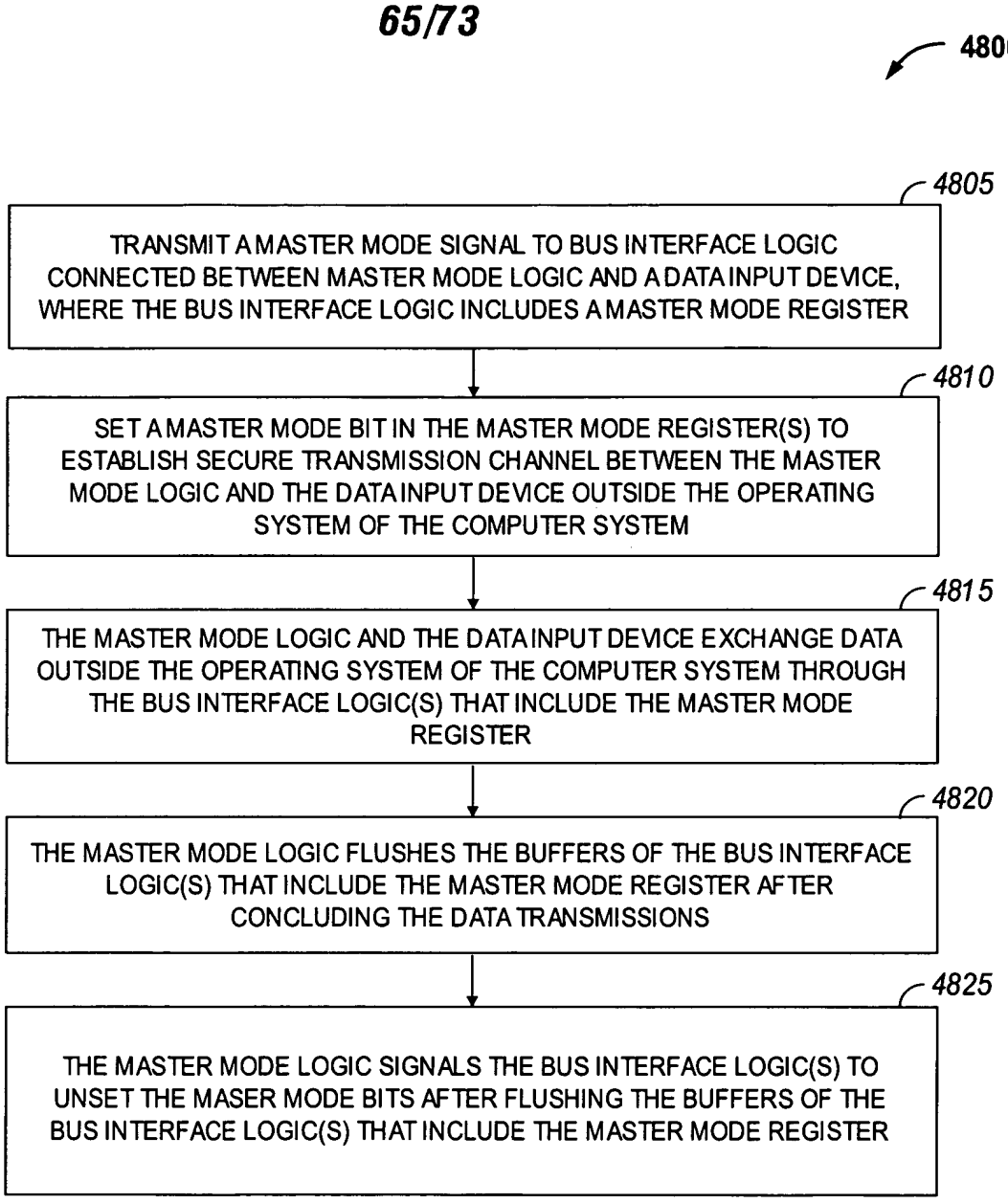
4800
4805
TRANSMIT A MASTER MODE SIGNAL TO BUS INTERFACE LOGIC CONNECTED BETWEEN MASTER MODE LOGIC AND A DATA INPUT DEVICE, WHERE THE BUS INTERFACE LOGIC INCLUDES A MASTER MODE REGISTER
4810
SET A MASTER MODE BIT IN THE MASTER MODE REGISTER(S) TO ESTABLISH SECURE TRANSMISSION CHANNEL BETWEEN THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM
4815
THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE EXCHANGE DATA OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM THROUGH THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER
4820
THE MASTER MODE LOGIC FLUSHES THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER AFTER CONCLUDING THE DATA TRANSMISSIONS
4825
THE MASTER MODE LOGIC SIGNALS THE BUS INTERFACE LOGIC(S) TO UNSET THE MASER MODE BITS AFTER FLUSHING THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER

FIG. 37

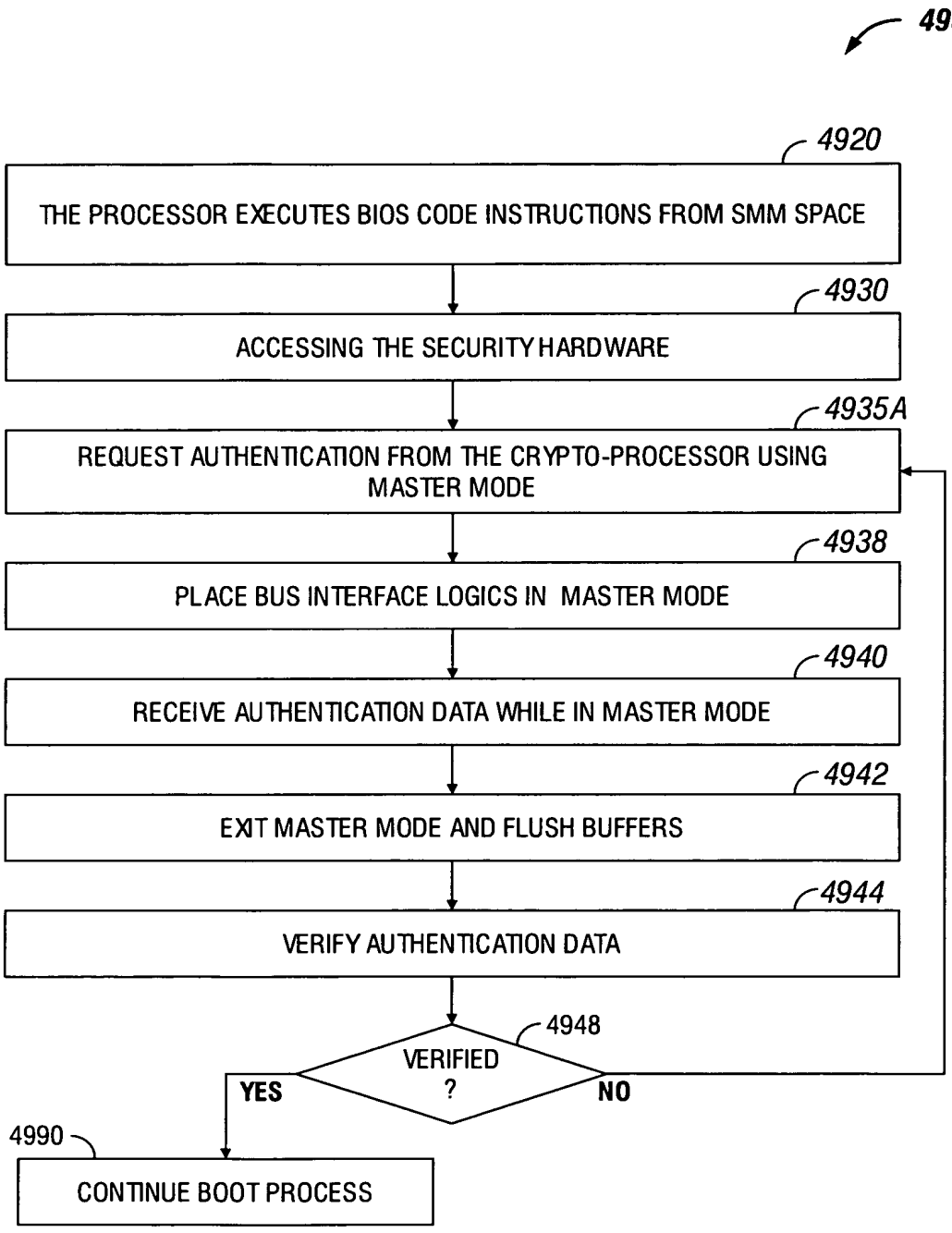
4900A
4920
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE
4930
ACCESSING THE SECURITY HARDWARE
4935A
REQUEST AUTHENTICATION FROM THE CRYPTO-PROCESSOR USING MASTER MODE
4938
PLACE BUS INTERFACE LOGICS IN MASTER MODE
4940
RECEIVE AUTHENTICATION DATA WHILE IN MASTER MODE
4942
EXIT MASTER MODE AND FLUSH BUFFERS
4944
VERIFY AUTHENTICATION DATA
4948
VERIFIED ?
YES
NO
4990
CONTINUE BOOT PROCESS

FIG. 38A

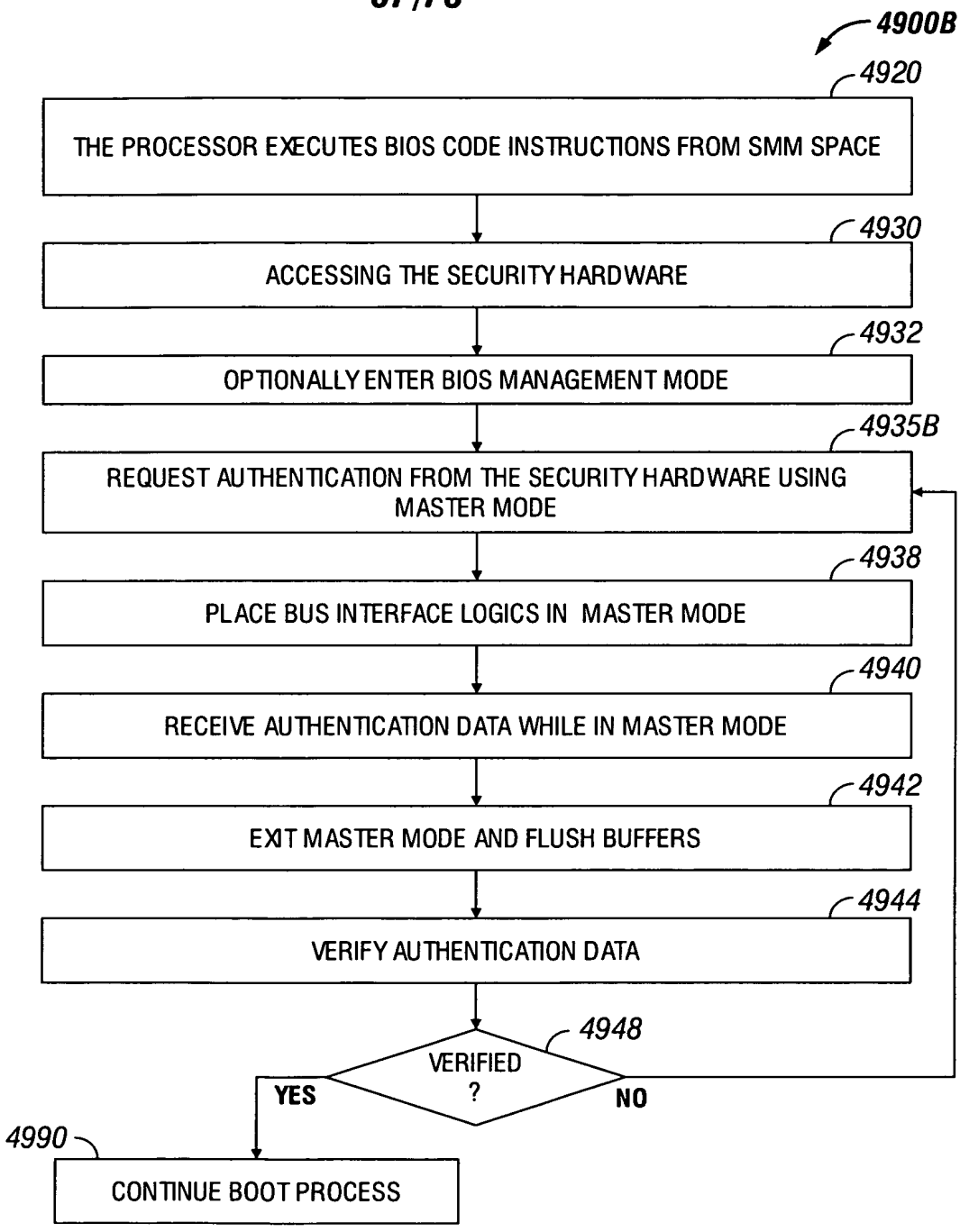
4900B
4920
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE
4930
ACCESSING THE SECURITY HARDWARE
4932
OPTIONALLY ENTER BIOS MANAGEMENT MODE
4935B
REQUEST AUTHENTICATION FROM THE SECURITY HARDWARE USING MASTER MODE
4938
PLACE BUS INTERFACE LOGICS IN MASTER MODE
4940
RECEIVE AUTHENTICATION DATA WHILE IN MASTER MODE
4942
EXIT MASTER MODE AND FLUSH BUFFERS
4944
VERIFY AUTHENTICATION DATA
4948
VERIFIED ?
YES
NO
4990
CONTINUE BOOT PROCESS

FIG. 38B

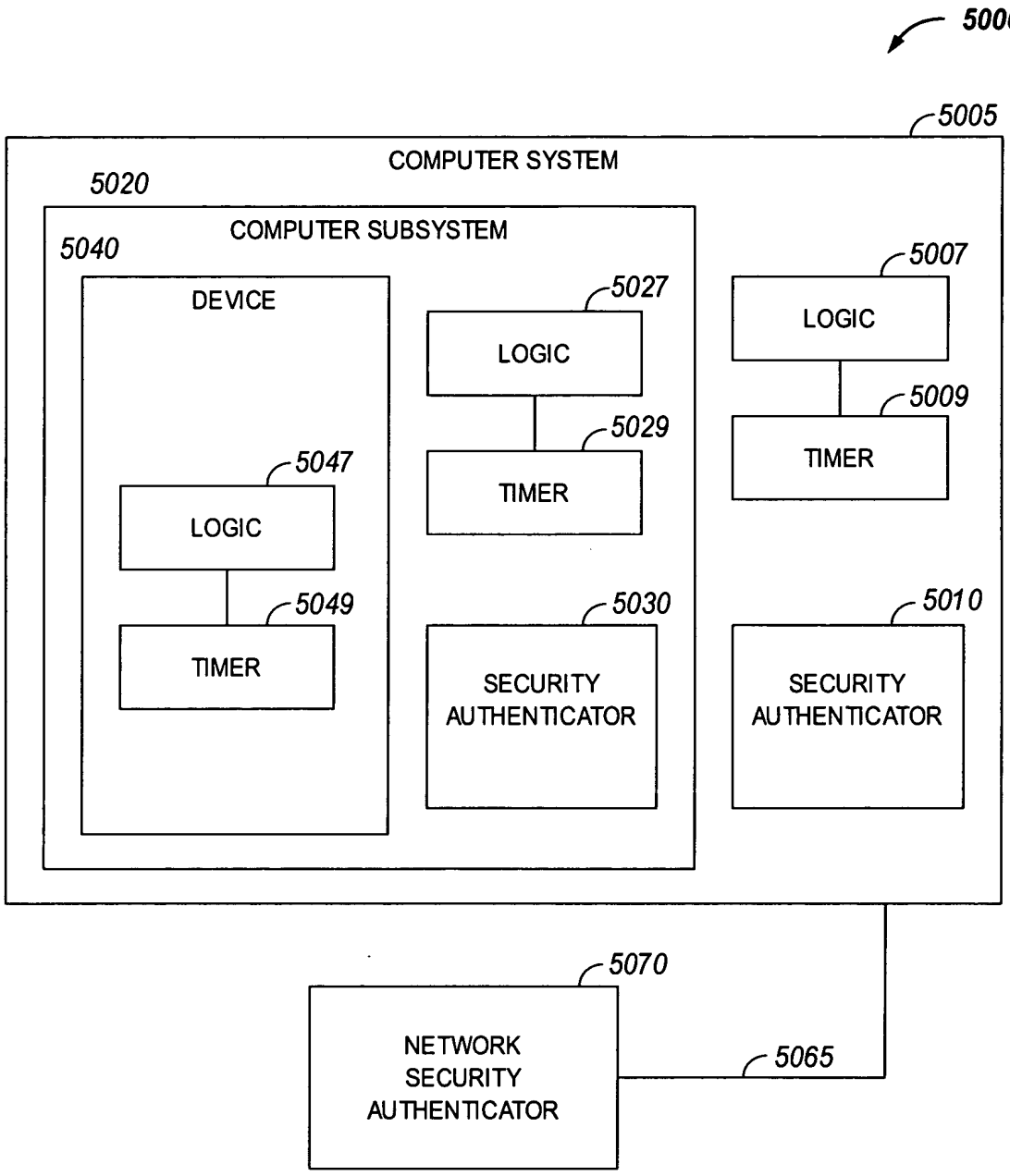
5000A
5005
COMPUTER SYSTEM
5020
COMPUTER SUBSYSTEM
5040
DEVICE
5047
LOGIC
5049
TIMER
5027
LOGIC
5029
TIMER
5030
SECURITY AUTHENTICATOR
5007
LOGIC
5009
TIMER
5010
SECURITY AUTHENTICATOR
5070
NETWORK SECURITY AUTHENTICATOR
5065

FIG. 39A

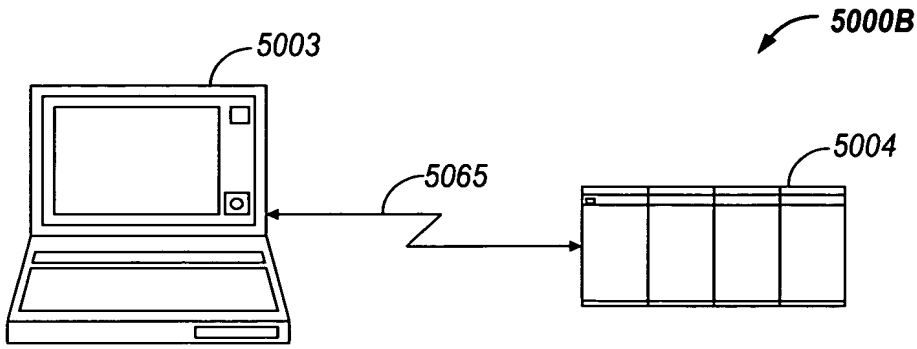

FIG. 39B

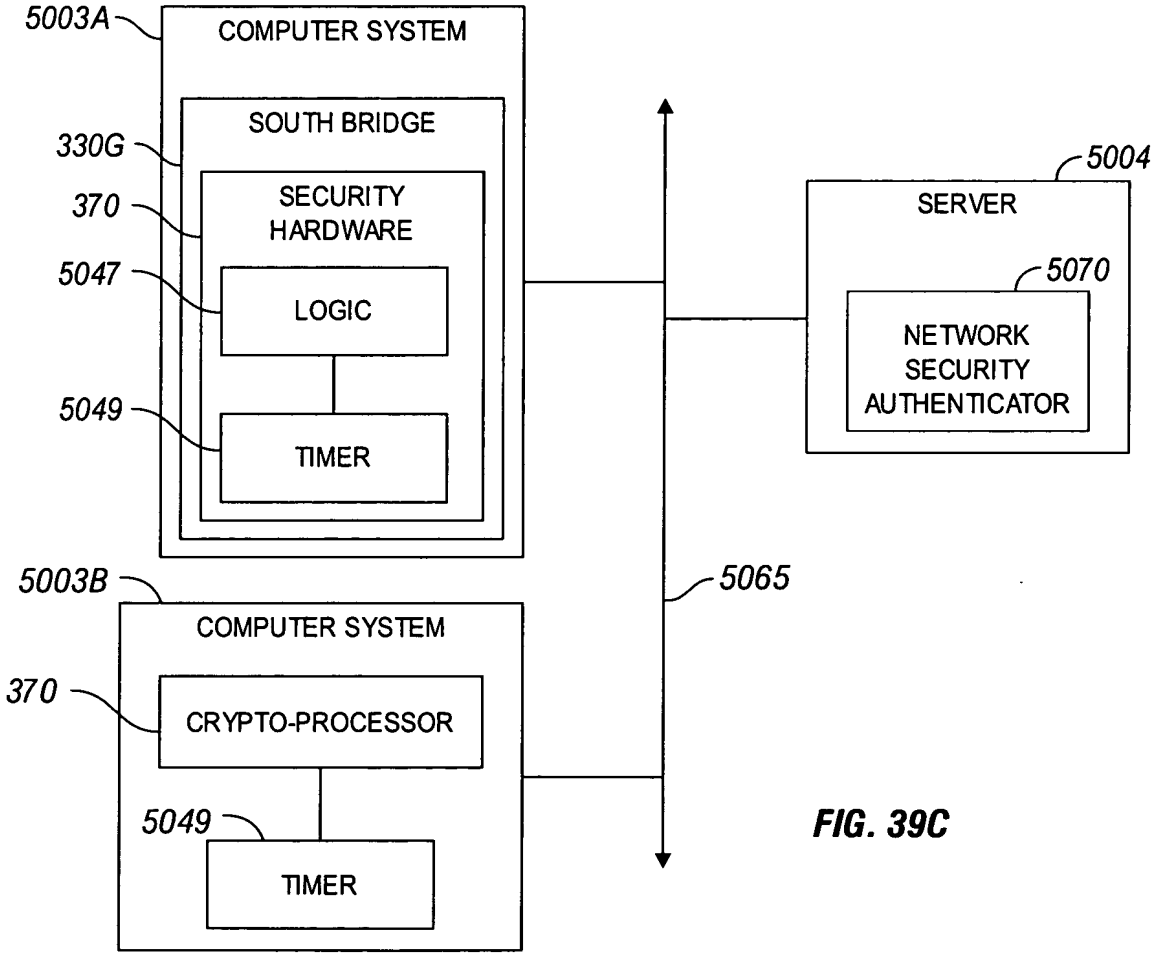

FIG. 39C

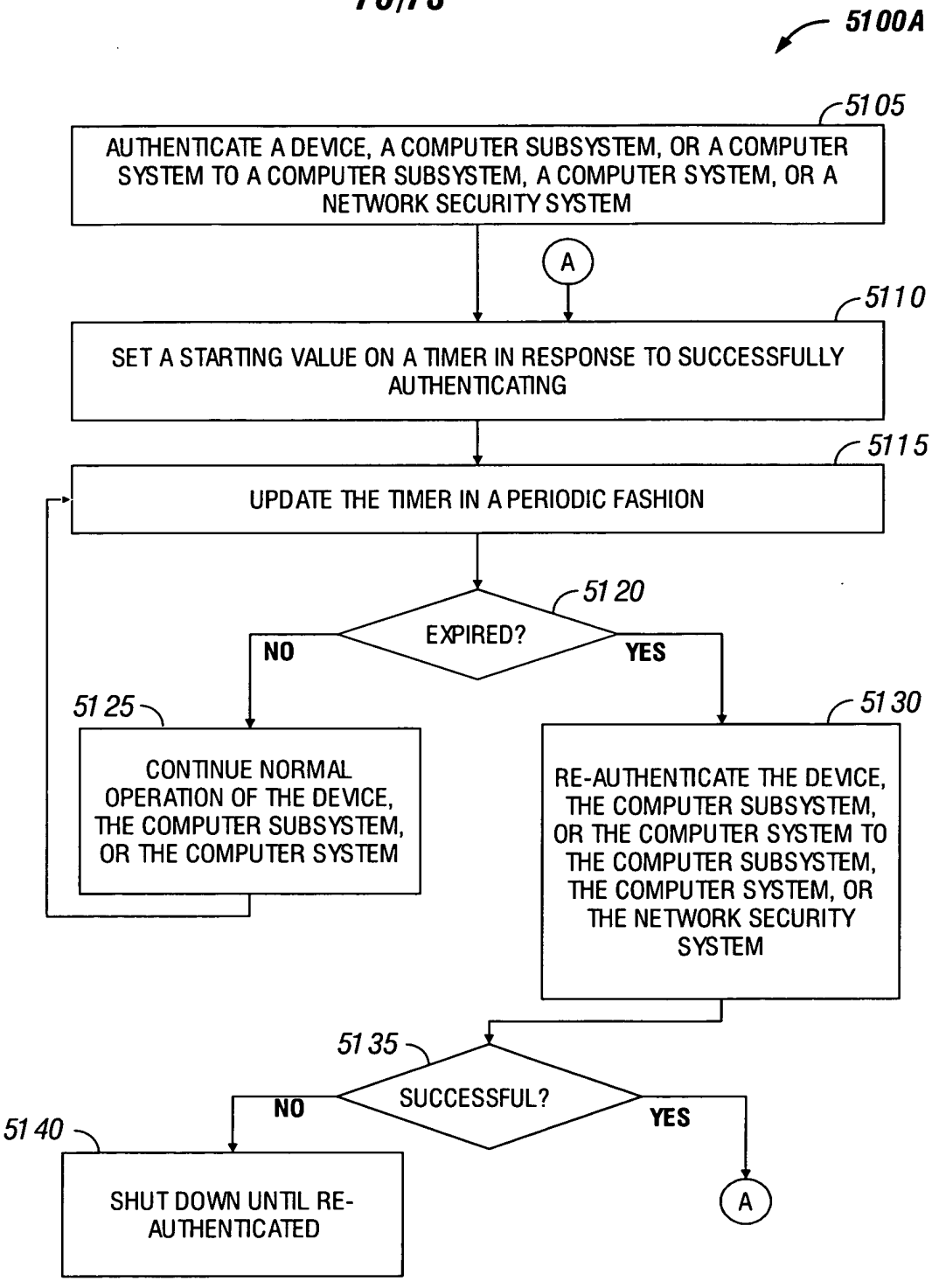
5100A
5105
AUTHENTICATE A DEVICE, A COMPUTER SUBSYSTEM, OR A COMPUTER SYSTEM TO A COMPUTER SUBSYSTEM, A COMPUTER SYSTEM, OR A NETWORK SECURITY SYSTEM
A
5110
SET A STARTING VALUE ON A TIMER IN RESPONSE TO SUCCESSFULLY AUTHENTICATING
5115
UPDATE THE TIMER IN A PERIODIC FASHION
5120
EXPIRED?
NO
YES
5125
CONTINUE NORMAL OPERATION OF THE DEVICE, THE COMPUTER SUBSYSTEM, OR THE COMPUTER SYSTEM
5130
RE-AUTHENTICATE THE DEVICE, THE COMPUTER SUBSYSTEM, OR THE COMPUTER SYSTEM TO THE COMPUTER SUBSYSTEM, THE COMPUTER SYSTEM, OR THE NETWORK SECURITY SYSTEM
5135
SUCCESSFUL?
NO
YES
5140
SHUT DOWN UNTIL RE-AUTHENTICATED
A

FIG. 40A

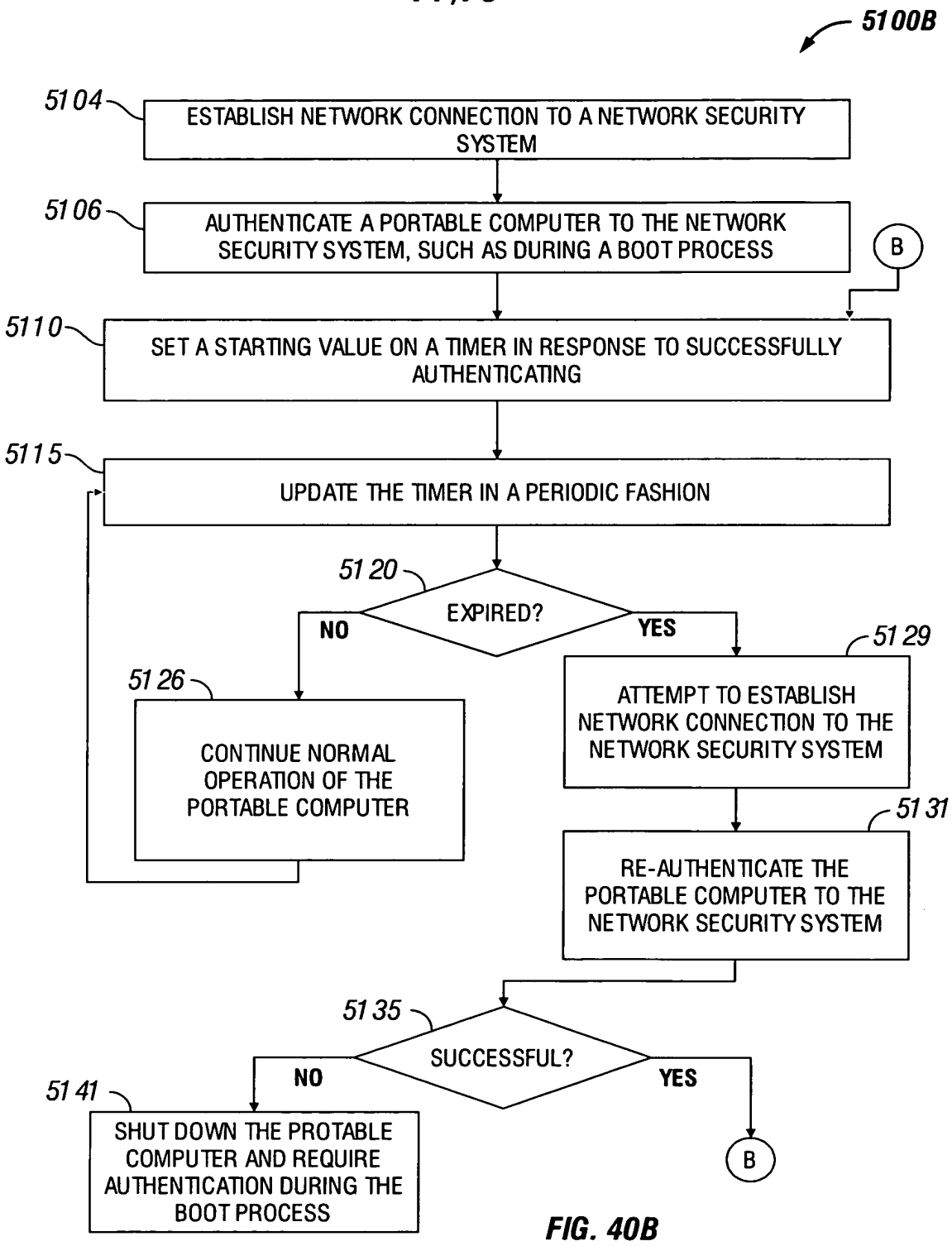
5100B
5104
ESTABLISH NETWORK CONNECTION TO A NETWORK SECURITY SYSTEM
5106
AUTHENTICATE A PORTABLE COMPUTER TO THE NETWORK SECURITY SYSTEM, SUCH AS DURING A BOOT PROCESS
B
5110
SET A STARTING VALUE ON A TIMER IN RESPONSE TO SUCCESSFULLY AUTHENTICATING
5115
UPDATE THE TIMER IN A PERIODIC FASHION
5120
EXPIRED?
NO
YES
5126
CONTINUE NORMAL OPERATION OF THE PORTABLE COMPUTER
5129
ATTEMPT TO ESTABLISH NETWORK CONNECTION TO THE NETWORK SECURITY SYSTEM
5131
RE-AUTHENTICATE THE PORTABLE COMPUTER TO THE NETWORK SECURITY SYSTEM
5135
SUCCESSFUL?
NO
YES
5141
SHUT DOWN THE PROTABLE COMPUTER AND REQUIRE AUTHENTICATION DURING THE BOOT PROCESS
B

FIG. 40B

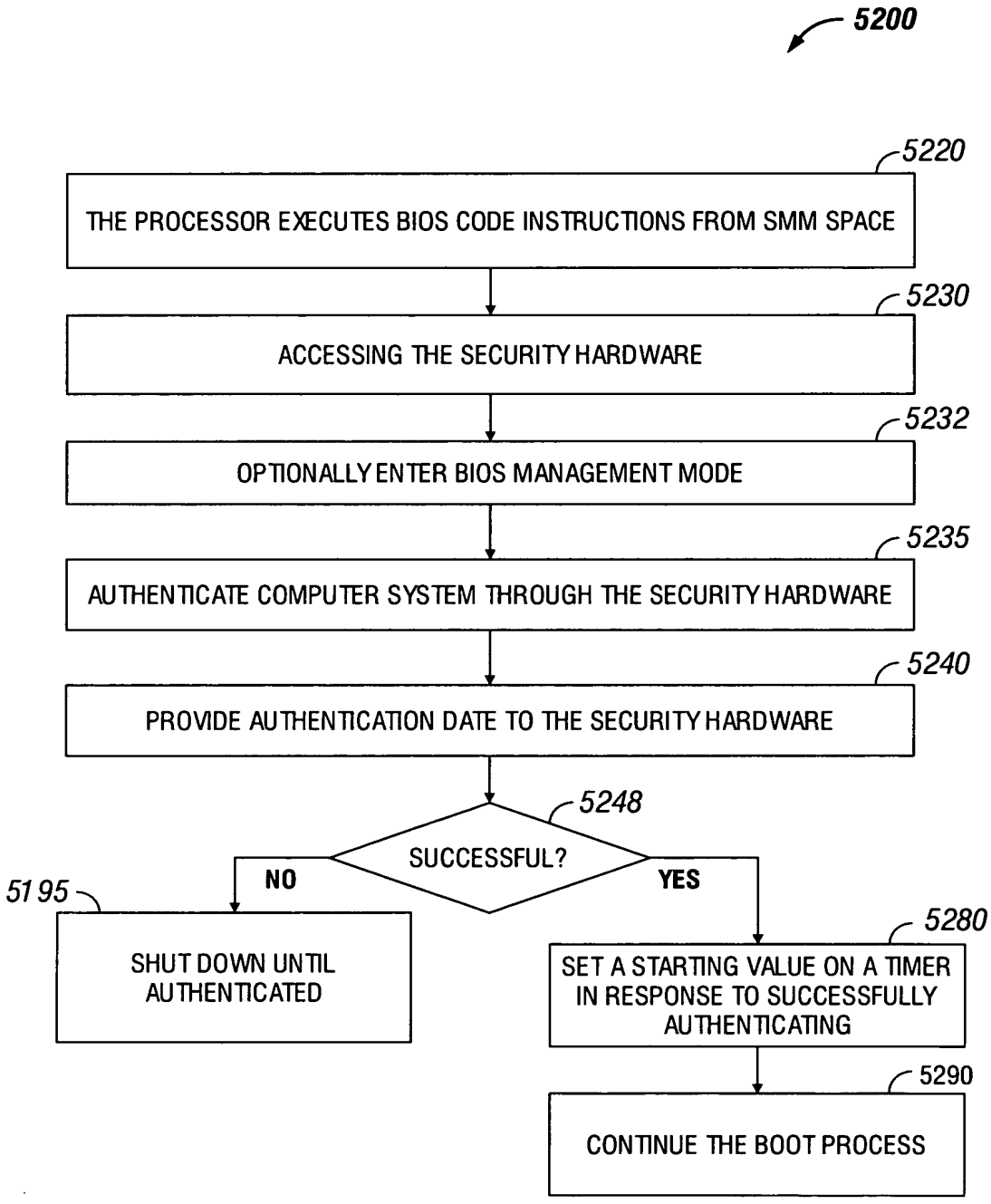
5200
5220
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE
5230
ACCESSING THE SECURITY HARDWARE
5232
OPTIONALLY ENTER BIOS MANAGEMENT MODE
5235
AUTHENTICATE COMPUTER SYSTEM THROUGH THE SECURITY HARDWARE
5240
PROVIDE AUTHENTICATION DATE TO THE SECURITY HARDWARE
5248
SUCCESSFUL?
NO
YES
5195
SHUT DOWN UNTIL AUTHENTICATED
5280
SET A STARTING VALUE ON A TIMER IN RESPONSE TO SUCCESSFULLY AUTHENTICATING
5290
CONTINUE THE BOOT PROCESS

FIG. 41

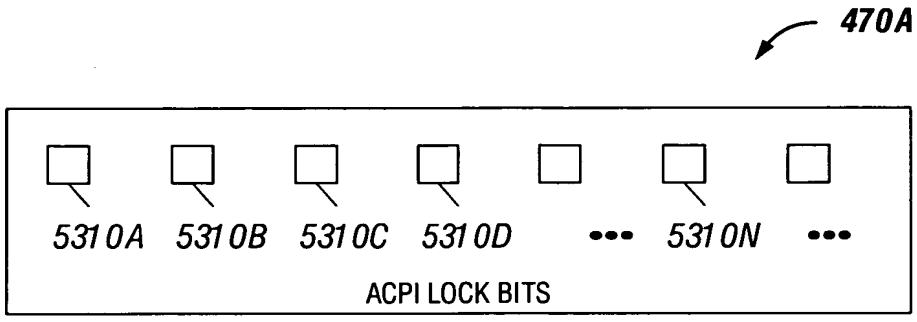

FIG. 42A

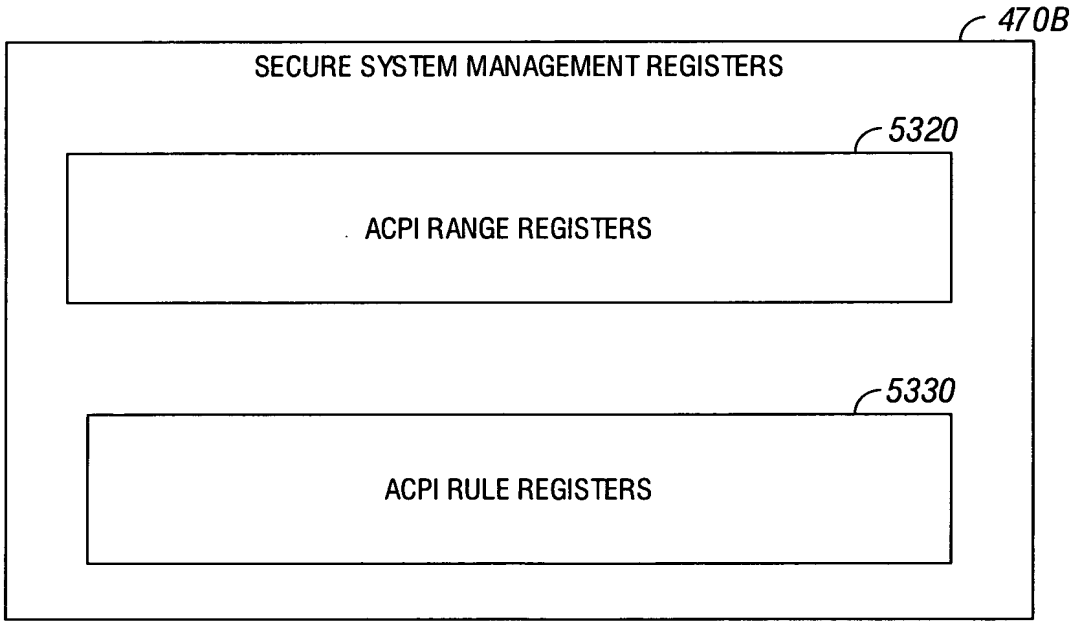

FIG. 42B